

KIEN5000/6000 Industrial Ethernet Switch Dedicated Network Management User's Manual

Beijing KYLAND Telecom Technology Co., Ltd.

KIEN5000/6000 Industrial Ethernet Switch dedicated Network Management User's Manual

Copyright © 2009 Beijing KYLAND Telecom Technology CO., LTD.

All rights reserved.

No part of this documentation may be excerpted, reproduced, translated, annotated or duplicated, in any form or by any means without the prior written permission of KYLAND Corporation.

Beijing KYLAND Telecom Technology Co., Ltd.

Address: Chongxin Mansion No.4 Building, 2nd Floor, Xijing Road 3#,

Shijingshan District, Beijing, China

Website: <http://www.kyland.cn>

Postcode: 100041

Tel: (+8610) 82900770

Fax: (+8610) 82900780

E-mail: sales@kyland.cn

Version: v3, Feb. 2009

Preface

KIEN5000 and KIEN6000 is high-performance network-managed industrial Ethernet switch specially designed by KYLAND Telecom Technology CO., LTD. for industrial applications. Its high-performance switch engine, solid and closed case design, high-efficient single-rib shape case heat dispersion surface without fans, over current, over voltage and EMC protection at power input side, and excellent EMC protection of RJ45 port allows KIEN5000 and KIEN6000 applicable in harsh and dangerous industrial environments. The redundant function of optical fiber network, independent entire network management channel, redundant power input function, and powerful entire network real-time management system provides multiplex guarantee for reliable operation of the system.

The *KIEN5000/6000 Industrial Ethernet Switch Dedicated Network Management User's Manual* mainly introduces the usage and operation of the network management and local configuration software in the KIEN5000 and KIEN6000 industrial Ethernet switch dedicated network management, and provides the reference for users to commence, expand and routine maintain the system. At the same time, it applies to the user training and learning for related technical personnel, so it is the practical teaching material for mass users to learn about the KIEN5000 and KIEN6000 industrial Ethernet switch-dedicated network management system.

This manual mainly includes the following contents:

Chapter 1 introduces general description and system features of KIEN5000 and KIEN6000 industrial Ethernet switch;

Chapter 2 introduces Network Management Operation Process of KIEN5000 and KIEN6000;

Chapter 3 introduces aggregate commands of KIEN5000 and KIEN6000;

Chapter 4 introduces WEB Network Management Operation Process of KIEN5000 and KIEN6000;

This document can be used together with the KIEN5000 Industrial Ethernet Switch-dedicated Network Management User's Manual and the KIEN6000 Industrial

Ethernet Switch-dedicated Network Management User's Manual.

Statement: For continuous update and perfection of the product and technology, the contents of this material may not be consistent with the actual product, please contact us about related contents. If it is necessary for you to query the latest information on the product, please query our Website or contact with your local service representative directly.

Safety Consideration

This product can provide excellent and reliable performance within its design scope. However, it needs to avoid the damage or destroy by human reasons.

- Read this Manual thoroughly and keep it well for future reference.
- Do not place the Device next to the source of water and the damp place.
- Do not place anything on the power cable. Please place where it cannot be reached.
- In order to avoid fire, do not tie or pack the cable.
- The connector of the power supply and other Device connection should be firmly connected and regularly checked.

Under following conditions, please power off and contact with our company immediately.

1. Water into Device;
 2. The Device is broken or the crust is cracked.
 3. The Device works abnormally or the performance provided has changed completely.
 4. The Device gives off odor, smoke or noise.
- Pay attention to the cleanness of the fiber socket and jack. When the Device operates, do not watch the end-face of the fiber directly.
 - Pay attention to the cleanness of the Device and clean it with soft cotton cloth if necessary.
 - Do not repair the Device by yourself unless it is definitely indicated in this manual.

Description of Warning Mark:

This manual uses two kinds of obvious warning marks to prompt users that more attention should be paid during operation. The meanings of these marks as follows:



Warning: The comment after this mark should be paid more attention, the incorrect operation will cause the switch to be damaged seriously or it will cause body injury for the operator.



Caution, Note and dangerous: Prompt where more attention should be paid.

Content

Chapter One System Overview.....	5
1.1 Product overview	5
1.2 Feature.....	5
1.3 Packing List and unpacking check.....	7
Chapter Two Console Management	8
2.1 Console	8
2.1.1 Serial Port RS232 Console.....	8
2.1.2 Telnet console.....	11
2.2 Console Management.....	12
2.2.1 Status and Counter	13
2.2.2 Switch Configuration	15
2.2.3 The Protocol Related Configuration.....	31
2.2.4 Restart Switch	40
2.2.5 Command Line.....	41
2.3 1K Xmodem software	42
Chapter Three Command of Port Console	43
3.1 System Configuration	43
3.2 Switch Configuration——Advanced.....	43
3.3 Port Control.....	44
3.4 Trunking.....	45
3.5 Filtering Data	46
3.6 VLAN.....	47
3.7 Spanning Tree	48
3.8 Sniffer.....	49
3.9 Table A	49
Chapter Four WEB Management.....	50

4.1 WEB Network Management	50
4.2 Port Status	51
4.3 Port Statistics.....	52
4.4 Administrator	53
4.4.1 IP Address	53
4.4.2 Configuration	54
4.4.3 Console Information.....	57
4.4.4 Port Control.....	57
4.4.5 Aggregator.....	58
4.4.6 Filter	60
4.4.7 VLAN.....	63
4.4.8 STP	67
4.4.9 Monitor Port.....	69
4.4.10 SNMP.....	70
4.4.11 Security	71
4.5 TFTP software.....	72
4.6 Backup	72
4.6.1 TFTP Restore Configuration	72
4.6.2 TFTP Backup Configuration	73
4.7 Reset.....	73
4.8 Reboot.....	76

Chapter One System Overview

1.1 Product overview

KIEN5000 AND KIEN6000 are two kind of high-performance managed industrial Ethernet switch specially designed by KYLAND Telecom Technology CO., LTD. for industrial applications. Its high-performance exchange engine, solid and closed case design, high-efficient single-rib shape case heat dispersion surface without fans, over current, over voltage and EMC protection at power input side, and excellent EMC protection of RJ45 port allows KIEN5000 AND KIEN6000 applicable in harsh and dangerous industrial environments. The redundant function of optical fiber network, independent full network management channel, redundant power input function, and powerful full network real-time management system provides multiplex guarantee for reliable operation of the system.

KIEN5000 and KIEN6000 industrial Ethernet switch provide two mounting ways, DIN rail and Wall-mounting.

On the front panel of KIEN5000, there are four uplink redundant 10Base-T/100Base-TX Ethernet RJ45 interfaces. The uplink redundant Ethernet RJ45 can be used to form two twisted-pair redundant ring networks. In the event of system failure, the recovery time of the redundant ring network should be less than 300ms.

On the front panel of KIEN6000, there is two pair of 100Base-FX single mode or multi-mode optical fiber interfaces. The uplink optical fiber interfaces can be used to form an optical fiber redundant ring network. In the event of system failure, the recovery time of the redundant ring network should be less than 300ms.

KIEN5000 and KIEN6000 provide four 10Base-T/100Base-TX RJ45 ports. Each RJ45 port has automatically adaptive function, capable of automatically configuring to 10Base-T or 100Base-TX status and full duplex or half duplex operation mode.

1.2 Feature

High-performance Industrial Ethernet Switch

1. 10/100Base-T/TX Ethernet ports, adaptive, full/half duplex, auto MDI/MDI-X connection

2. 100Base-FX fiber ports, single mode/multimode, full duplex
3. High speed redundant ring with recovery time < 300ms
4. Supports VLAN to control broadcasting domain and segment flow.
5. Alarms relay output power supply and port link.
6. Broadcast storm control

Powerful Management Function

1. Integral management platform for the entire network based on RS232 standard. The management system is immune against the attack of virus or hacker since the management channel is independent to service channel.
2. Special-designed management software for upper PC realizes the auto-configuration of IP address for networking devices and auto-scan/spanning of network topology.
3. Individual naming for each device in the network.
4. Setting and query of VLAN.
5. Setting and query for alarm of power and ports link.
6. Setting and query for port working mode, prioritization, and rate

Industrial Power

1. Industrial power input of DC24V (DC18V~36V) .
2. Reliable protection for EMC and against over-current/over-voltage.
3. Redundant power input.

Rugged Design

1. Ribbed heat-removal design (fan less); operation at -35°C to +75°C
2. Solid IP40 housing
3. Easy DIN-Rail mounting or optional wall-mounting

1. 3 Packing List and unpacking check

1 . Packing List

The packing case includes the following items:

KIEN5000 (or6000)	1 unit
3-core DC power terminal	2 pieces
2-core alarming output terminal	1 piece
User's Manual for KIEN5000 (or6000) Industrial Ethernet Switch	1 copy
Customer Service Guideline	1 copy
Φ3 grounding cold pressed terminal, M3×8 grounding screw	1 piece each

2 . Unpacking check

Before opening the case, place it stably, pay attention to the direction of the packing case, and ensure its right side is facing upward, so as to prevent KIEN5000 AND KIEN6000 from falling apart after opening the case. If a hard object is used to unclench the case, do not overly extend the hard object into the case to avoid damage of the equipments inside the case.

After opening the case, check the amount of KIEN5000 AND KIEN6000 equipments (including main unit of KIEN5000 AND KIEN6000, parts of equipment, user's manual, customer service guideline) according to the packing list, and check the appearance quality of KIEN5000 AND KIEN6000.



Warning:

For the built-in precise parts of equipments, please handle with care and avoid strenuous vibration to avoid affecting the performances of equipments.

Chapter Two Console Management

2. 1 Console Login

2. 1. 1 Login RS232 Serial Port Console

You can login the RS232 serial port console software from hyper terminal of WINDOWS system, and realize the query, configuration and management in KIEN5000/6000. If there is no such a software in the system, you can install it from “Add/Delete Program”, afterwards, you can login as following:

1. To connect the RS232 console port of KIEN5000/6000 with PC's serial port(ex: COM1 or COM2 depending on the PC's serial port hardware and its occupation status.) by serial port cable (from RJ45 to DB-9F/DB-25F).
2. Click “Star” → “All programs”→“Accessories”→“Communications” → “Hyper Terminal”.

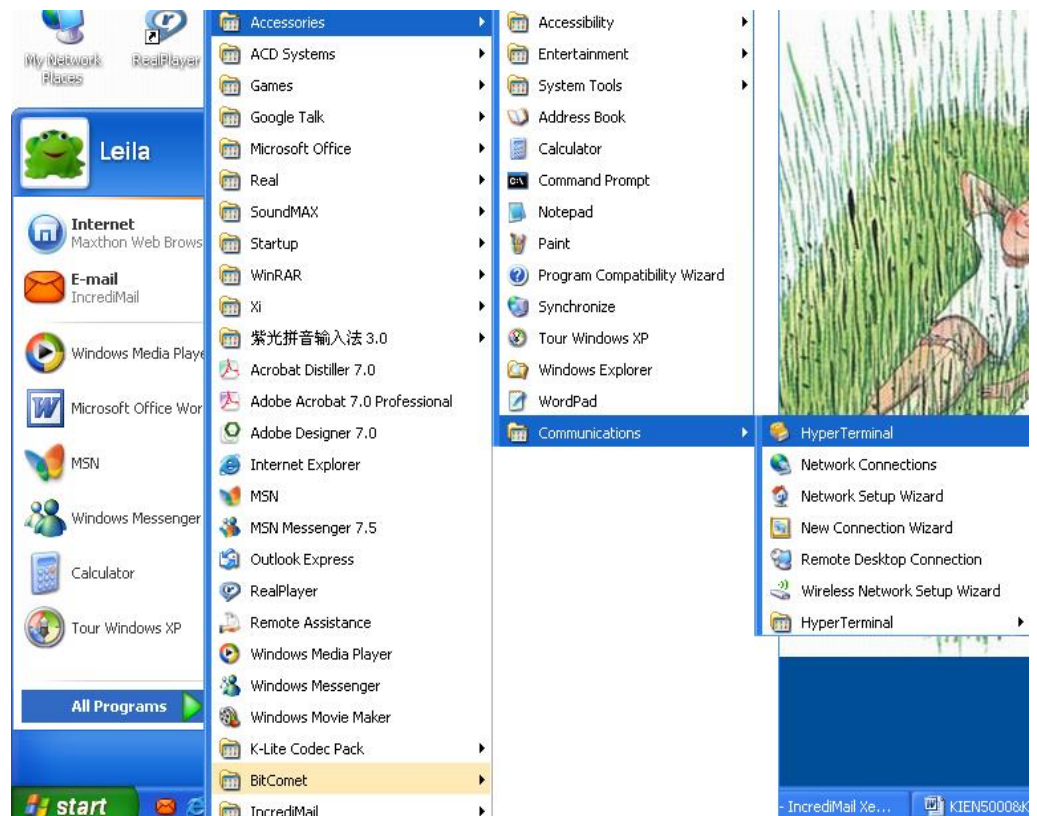


Figure2-1 Login Console Management

3. The following figure shows “New Connection” dialog box. For

example : “COMMON1” and then click “OK”.



Figure2-2 Connection

4. To select serial port according to the PC's serial port hardware and its occupation status. For example, to select “COM1” and click “OK”.



Figure2-3 Select port

5. As the following shows, to set the properties of “COM1” : Bits Per Second:9600bps; Data bits: 8 ; Parity: None; Stop bits: 1 ; Flow Control: None, click “OK” to enter the console interface.

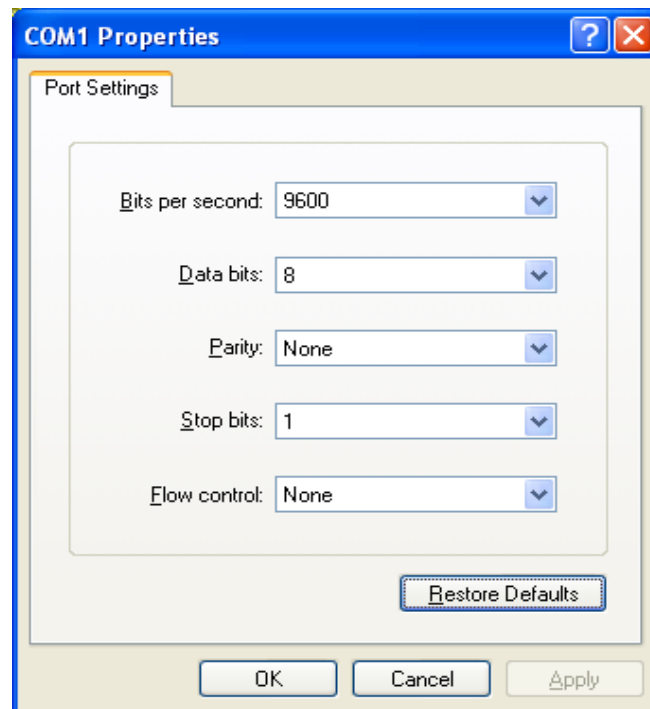


Figure2-4 Port Setting

6. The console interface is shown as below. To enter Username: admin → <Enter>; Password :123→<Enter>, and enter the main menu.

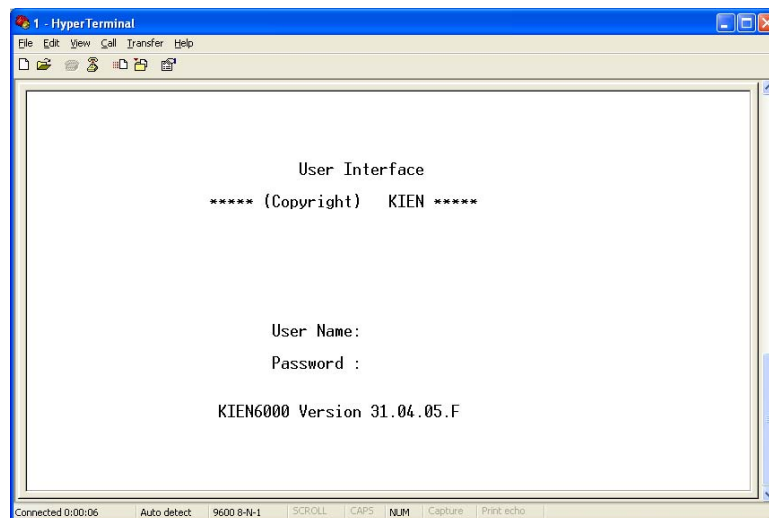


Figure2-5 Login Console

7. The main menu is shown as below, when in the menu, all operation should be realized by the keyboard, the direction is as below:

Table2-1 Direction of Keyboard for menu

Key	Function
<Tab>:	Go to next item;
<Backspace>:	Go to previous item;
<Enter>:	Pitch on and enter the item;

<Space>:	Convert current item's configuration
<Ctrl>+A:	Implement current operation

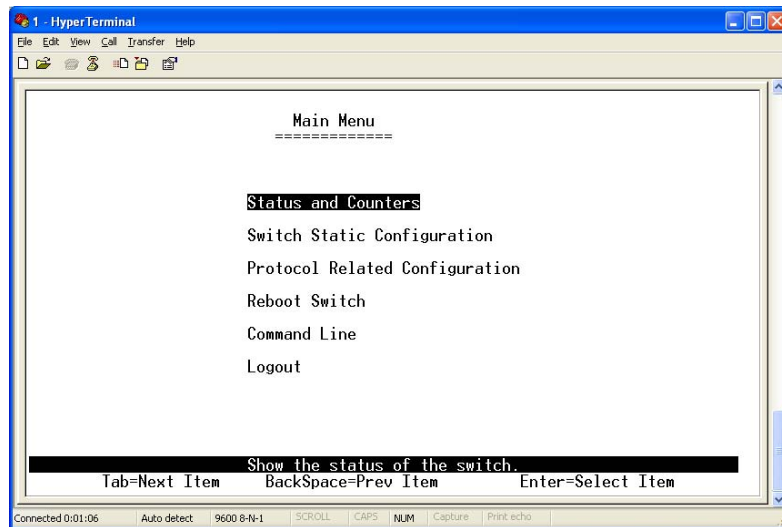


Figure2-6 RS232 Console Menu

2. 1. 2 Telnet console

You can also visit the console software of KIEN5000/6000 from network by Telnet way. In this way, you need to connect any one of RJ45 ports of KIEN5000/6000 with the Ethernet port in the network or the PC's card by a cross-over or straight-through copper cable. You can do as follows:

1. Windows → “Run” or MS-DOS command line, to enter the login page.

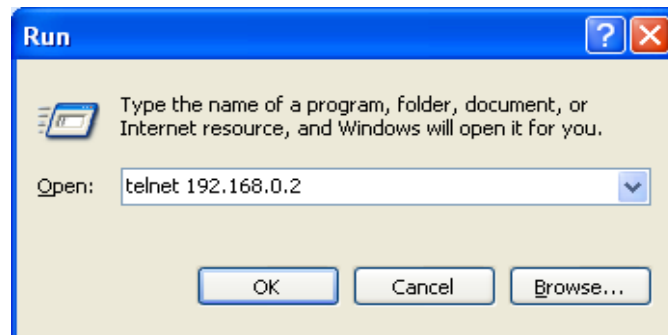


Figure2-7 Run Telnet

2. Username : admin → <Enter>, Password:123 → <Enter>, KIEN5000 or KIEN6000's Telnet Console Management Main Menu.

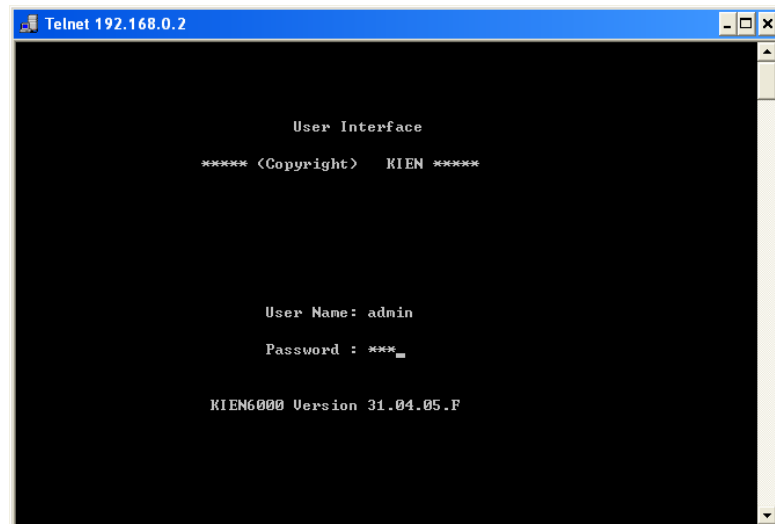


Figure2-8 Login Telnet

3. The following figure shows the Main Menu, all operations are realized by keyboard, whose detailed function is the same as RS232 console's.

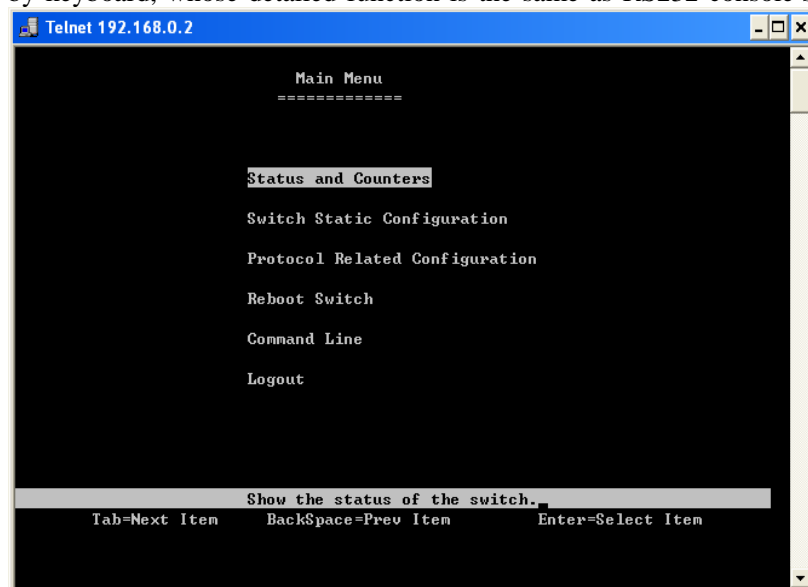


Figure2-9 Main Menu

2. 2 Console Management

There are two kind of way login the Console Management, one is RS232 Console and another one is Telnet such as Figure 2-6 and Figure 2-9. Their operations and functions are the same. So the following introductions to the menus are for both managements.



Attention:

KIEN5000 and KIEN6000's default IP address is 192.168.0.2 , which can be referred to the coding label on the device.

Do not apply the two ways: Telnet Console and RS232 Console at same time!

Port 9 and 10 in the management is for the configuration of other products in the system, you can make configuration in the available items and ignore if any is not available.

2.2.1 Status and Counter

The following figure shows “Status and Counter”.

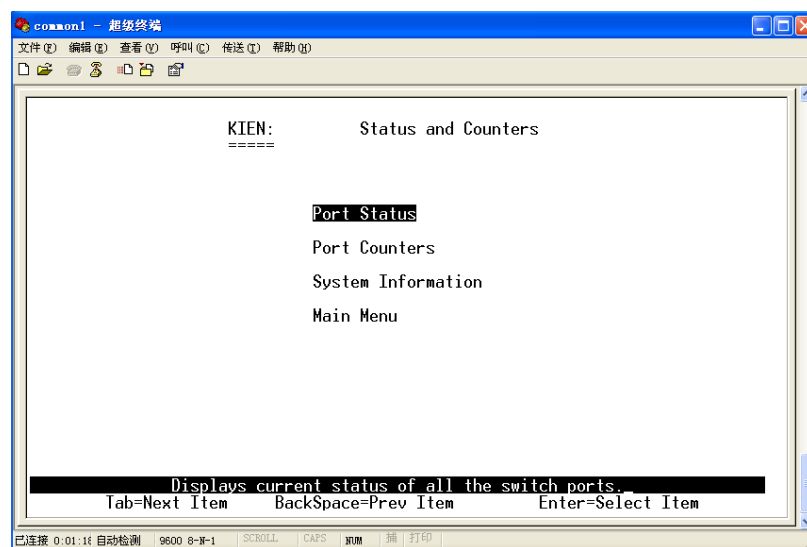


Figure2-10 Status and Counters

1. Port Status

The page of port status is shown as below, it shows the status of each port.

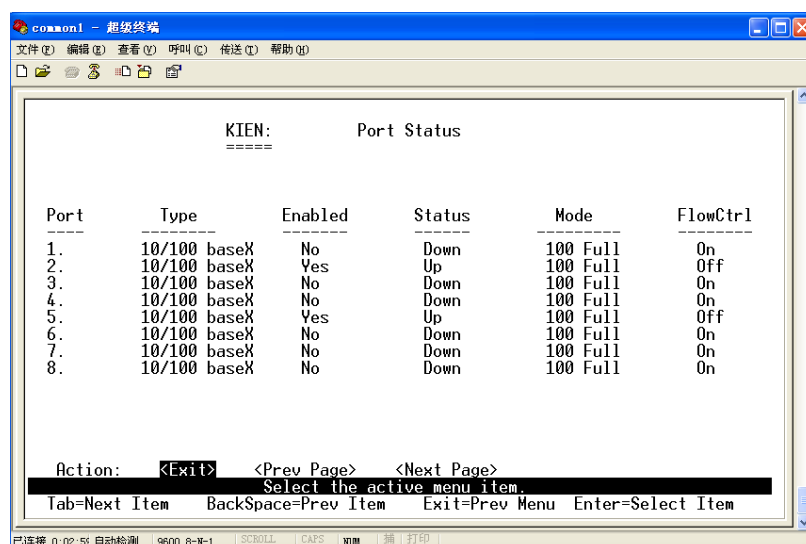


Figure2-11 Port Status

Table2-2 Port Status

Entry	Description
Type	Type of Port.
Enabled	It's enabled or disabled according to user configuration.
Status	Shows port connected or disconnected..
Mode	Shows port rate and duplex mode.
FlowCtrl	Shows flow control enabled or disabled.

2. Port Counter

The following page shows device's communication status.

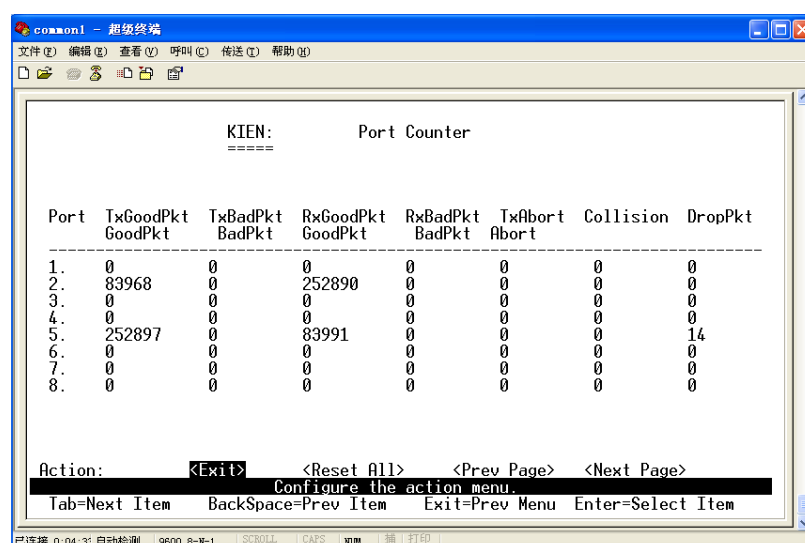


Figure2-12 Port Counter

3. System Information

The following page shows the software and hardware information of current system.

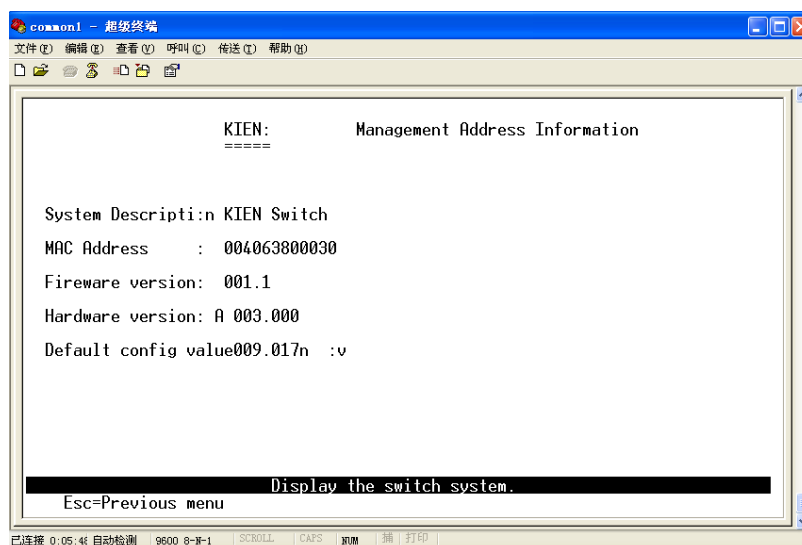


Figure2-13 Management Address Information

2. 2. 2 Switch Static Configuration

“Switch Configuration” → <Enter>.

“Switch Configuration” → “Administration Configuration”、“Port/Trunk Configuration”、“Port Mirroring Configuration”、“VLAN Configuration”、“Priority Configuration”、“MAC Address configuration”、“Misc Configuration”. You can select item using by <Tab> and <Backspace>. The seven next menus is introduced as following:

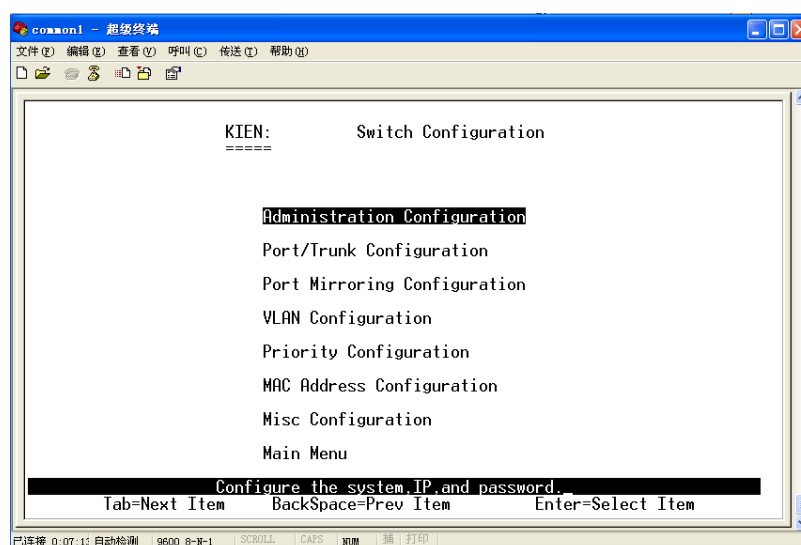


Figure2-14 Switch Configuration

2. 2. 2. 1 Administration Configuration

“Switch Configuration” → “Administration Configuration” → <Enter>. It’s including “Device Information”、 “IP Configuration”、 “Change Username”、 “Change Password”、 “MAC Configuration”.

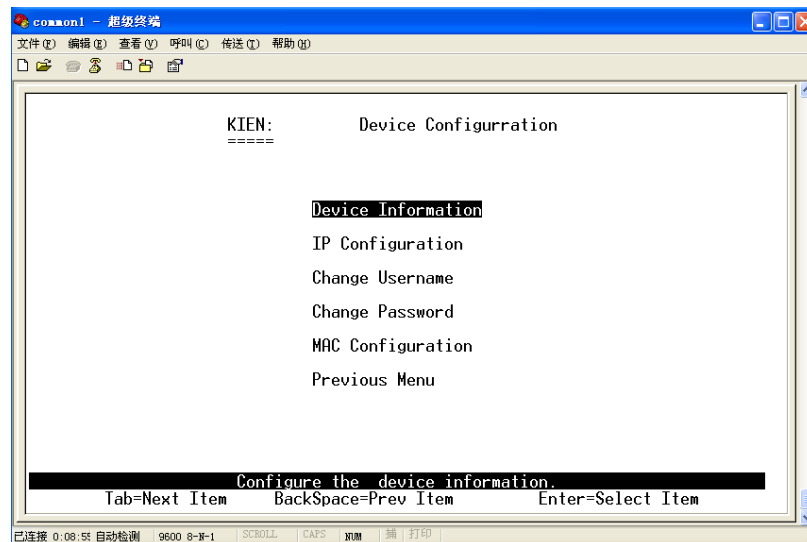


Figure2-15 Device Configuration

1. Device Information

The following figure shows device information. It’s including Device Name, Device Content, device Location, and Device description.

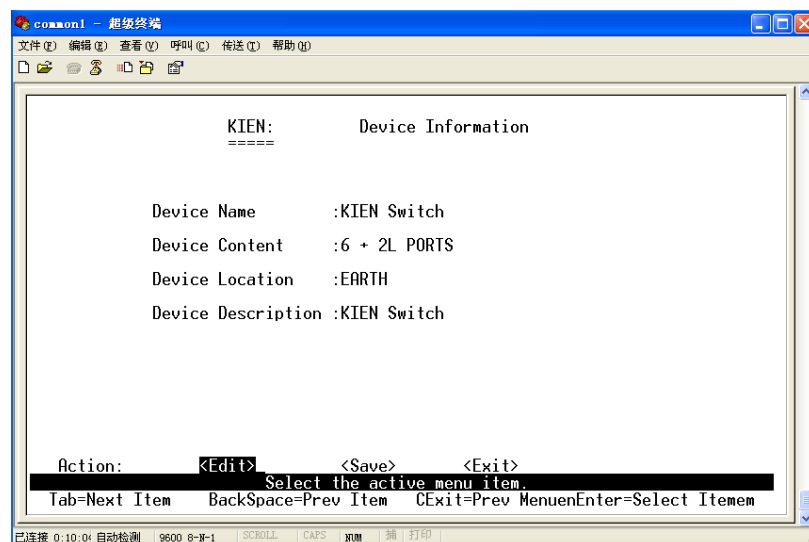


Figure2-16 Device Information

2. IP configuration

The following figure shows IP configuration. It’s including IP Address、 Subnet Mask、 Gateway.

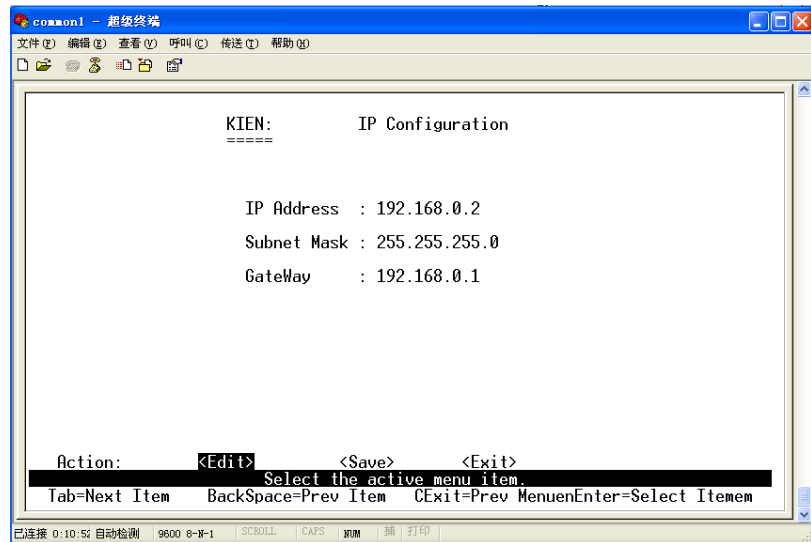


Figure2-17 IP configuration

3. Change Username

The following figure shows user configuration.

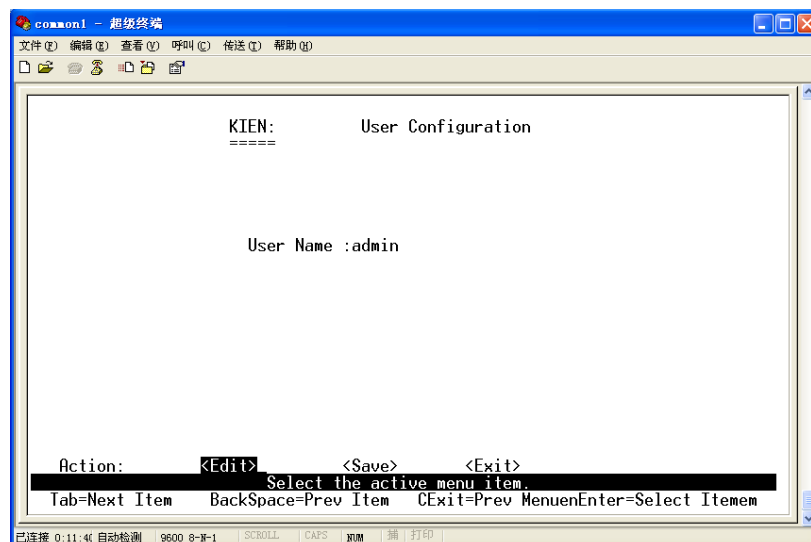


Figure2-18 User configuration

4. Change password

The following figure shows password configuration.

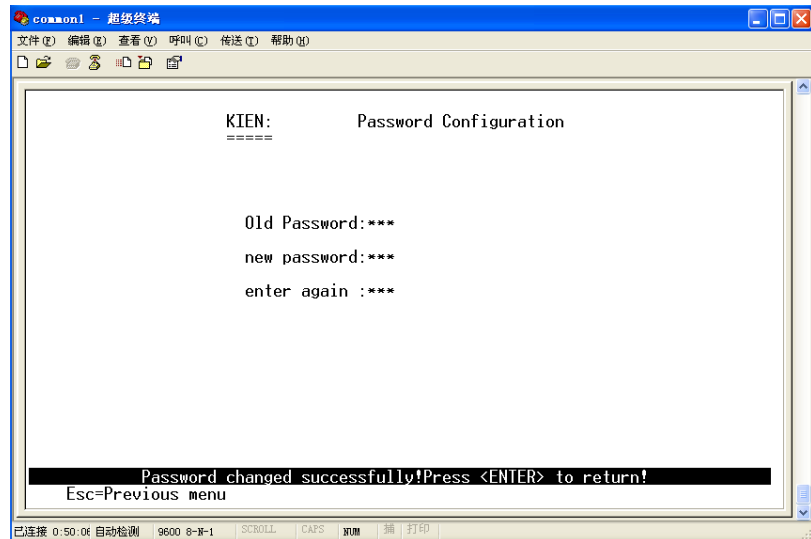


Figure2-19 Password Configuration

5. MAC Configuration

You can change MAC address of KIEN5000 or KIEN6000 Industrial Ethernet Switch in the following page.To avoid a conflict among the networking devices, you are suggested not to change it unless it is a must.

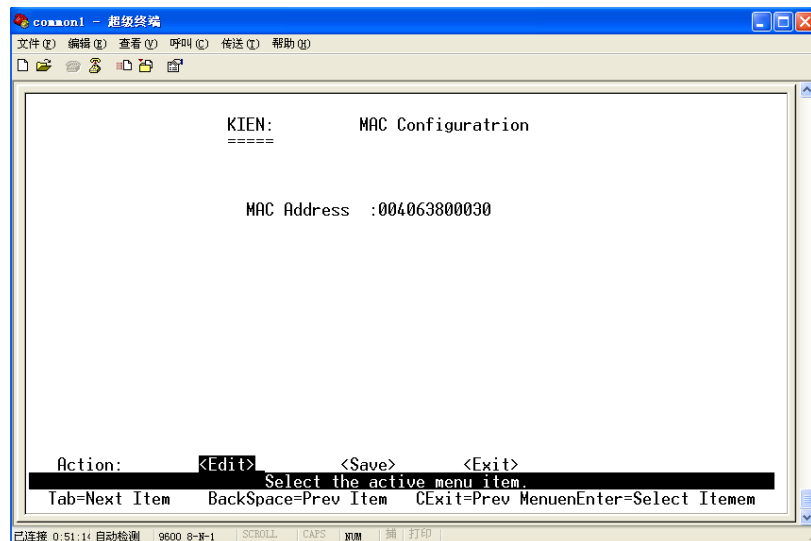


Figure2-20 MAC Configuration

2. 2. 2. 2 Port/Trunk Warning Configuration

“Switch Configuration” → “Port/Trunk Configuration” → <Enter>

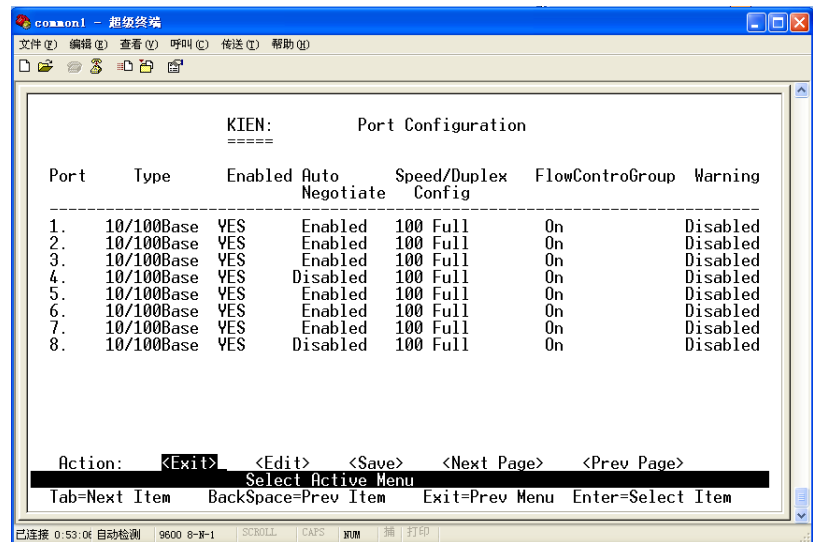


Figure2-21 Port Configuration

The above page shows port configuration and trunk group. You can convert the item by “space” key. The following table shows description of items.

Table2-3 Port/Converge/Alarm

Items	Description
Enabled	Enable or disable the port.
Auto Negotiate	Enable or disable auto-negotiation function for each port.
Speed/Duplex Config	Set the speed as 10Mbps or 100Mbpsand, and full duplex mode or half duplex mode.
Flow Control	Enable or disable the flow control function.
Group	Set the trunk group for ports.. There are four groups for configuration
Warning	Enabled or disable warning function.

2. 2. 2. 3 Port Mirroring configuration

“Switch Configuration” → “Port Mirroring Configuration” →<Enter>.

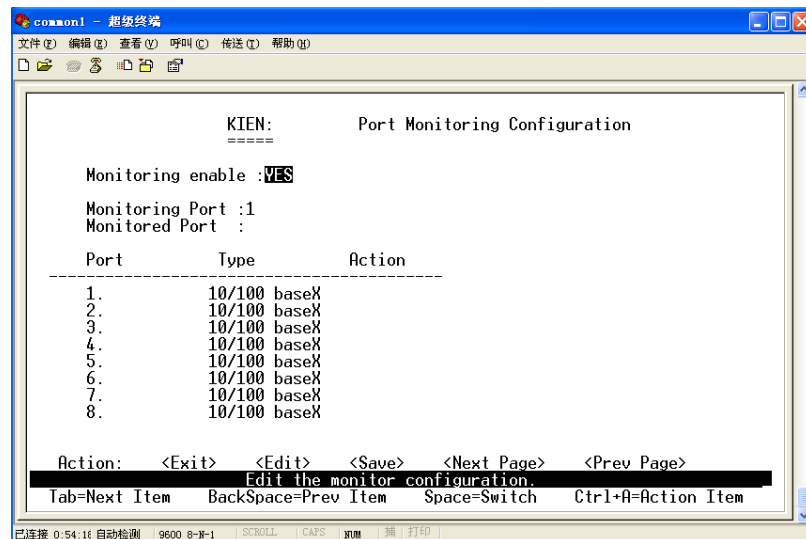


Figure2-22 Port Mirroring Configuration

Port mirroring is a way to monitor the network flow in the switching network. The port's flow can be monitored from a given port. The targeted flow will be copied to the mirroring port. Each item has the meaning as below:

Table2-4 Port Mirroring Configuration

Item	Description
Monitoring Enable	Enabled or disabled monitoring function.
Monitoring Port	Sniffer port to monitor all port communication.
Action	Ports to be monitored. The flow of all monitored ports are copied to the sniffer port. You can select up to 7 monitored ports in the switch. From the Action item, you can make choice to monitor the receiving frame, transmitting frame or both.

2. 2. 2. 4 VLAN Configuration

“Switch Configuration” → “VLAN Configuration” → <Enter>. It's including “VLAN Configuration”、 “Create a VLAN Group”、 “Edit/delete a VLAN Group”.

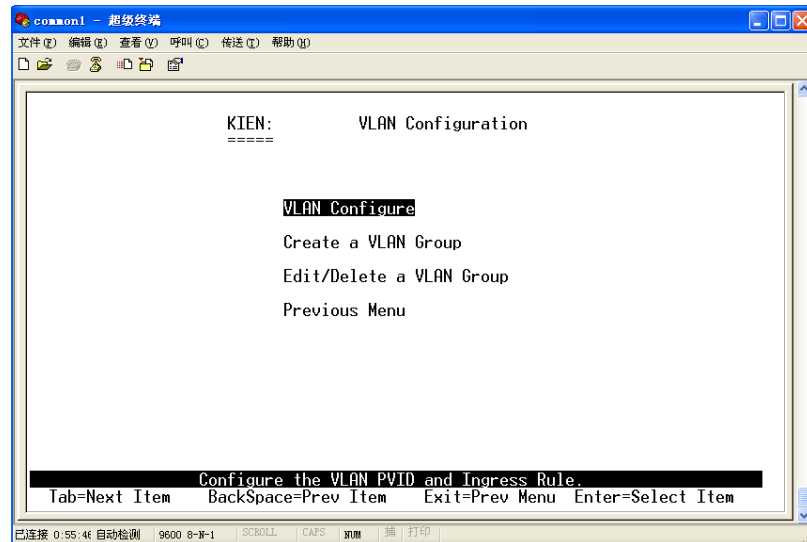


Figure2-23 VLAN configuration

1 . VLAN Support Configuration

The following page is for VLAN support configuration. It's including VLAN ID of each port and ingress rule of data packets.

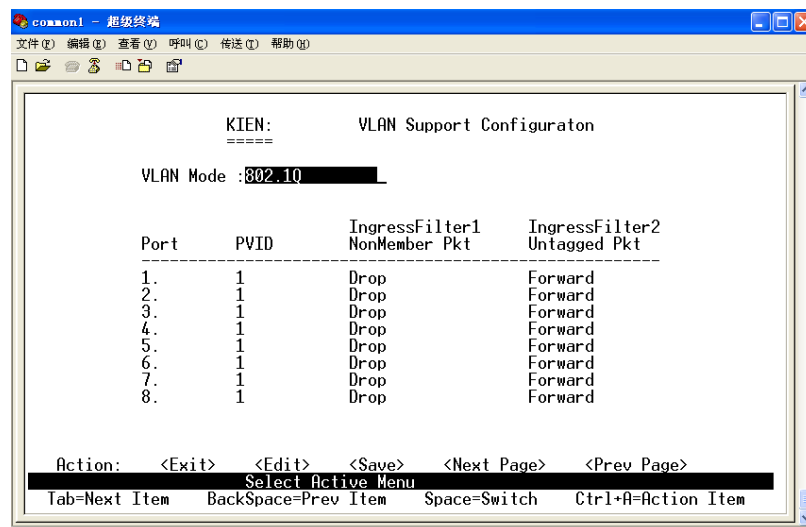


Figure2-24 VLAN Support Configuration

Table2-5 VLAN Support Configuration

Item	Description
VLAN Mode	By pressing “Space” key, you can convert three modes of port-based、802.1Q with GVRP、802.1Q without GVRP.
PVID	To set the VLAN ID of untagged flow of the given port. Ex: if port 3’s default PVID is 100, all the untagged packets of port 3 belong to VLAN 100. All ports’ default PVID is 1. This feature is applicable when you adjust the tag-unsupported device and want to add it to VLAN. Only one untagged VLAN is permitted in

	each port.
Ingress Filter 1 Nonmember Packet	This configuration is in line with ingress filter rule 1 of Web-management. Only the packet that is in line with port's VID. You can press "Space" key to forward or abandon the packets that do not comply with the VID setting.
Ingress Filter 2 Untagged Packets	This configuration complies with the ingress filter rule 1 of Web-management: to abandon the untagged frame. You can press "Space" key to forward or abandon the untagged frame.

2 . Create a VLAN Group

You can create VLAN from this page and add tagged/untagged member port. The following table 2-6 shows description of items.

Table2-6 Port of VLAN

Items	Description
VLAN Name	Input new VLAN name.
VLAN ID	Input VLAN ID (2~4094), Default is 1.
VLAN Protocol	Press "Space " key to select VLAN protocol type.
Member	Press "Space" key to select VLAN member. There are three kind of VLAN member: Tagged: The port belongs to tagged number. Untagged: The port belongs to untagged number. No: The port not belongs to the VLAN number.

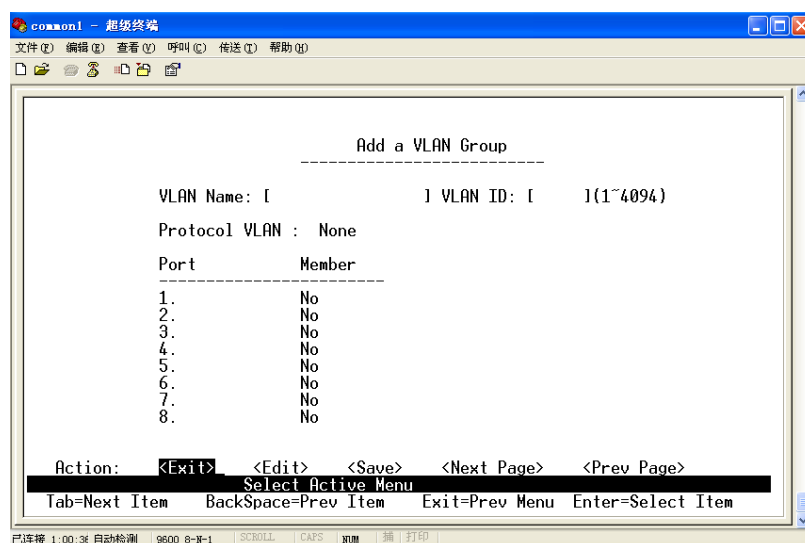


Figure2-25 Add a VLAN Group

3 . Edit/DeleteVLAN

You can edit or delete VLAN as followed:

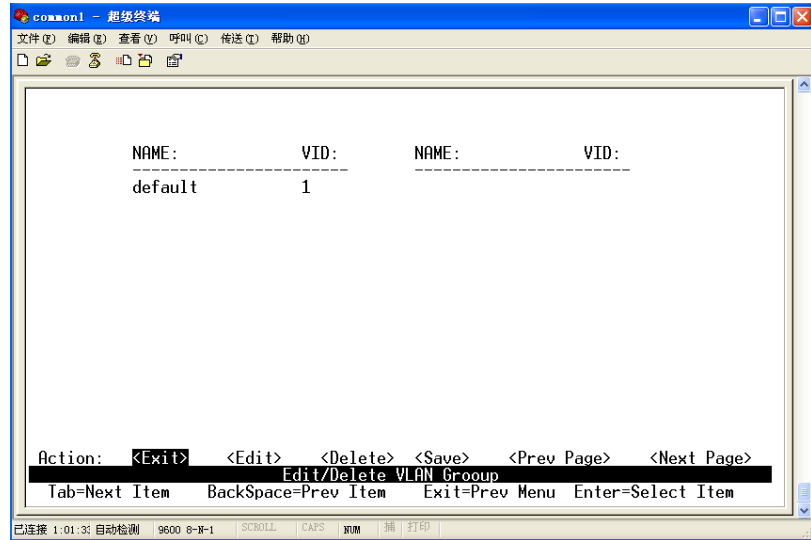


Figure2-26 Edit/Delete VLAN

- 1) Select VLAN to edit or delete, and press <Enter>.
- 2) You can change VLAN protocol item, change the member port between untagged and tagged, and delete some member port in VLAN group.
- 3) After editing or deleting VLAN, press<Save> and <Enter> to keep all the configurations.

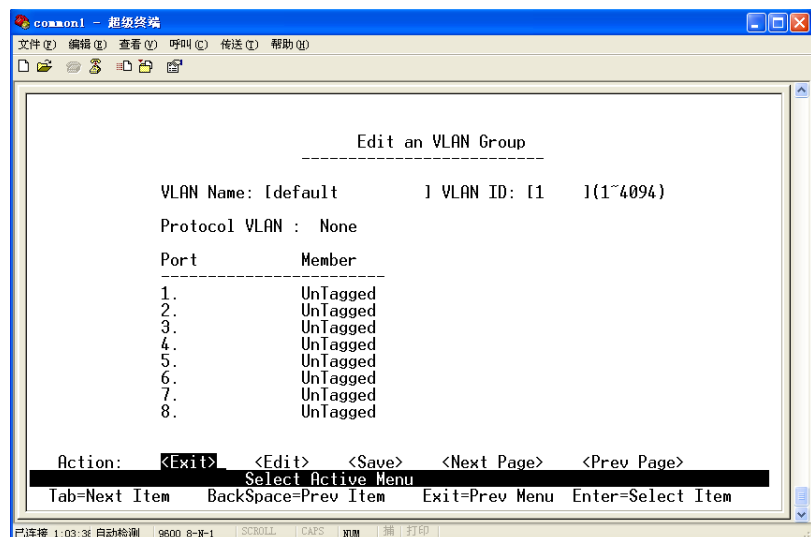


Figure2-27 Edit a VLAN Group



Attention:

VLAN name and VLAN ID cannot be changed. Default VLAN cannot be deleted.

2. 2. 2. 5 Priority Configuration

“Switch Configuration” → “Priority Configuration” → <Enter>.

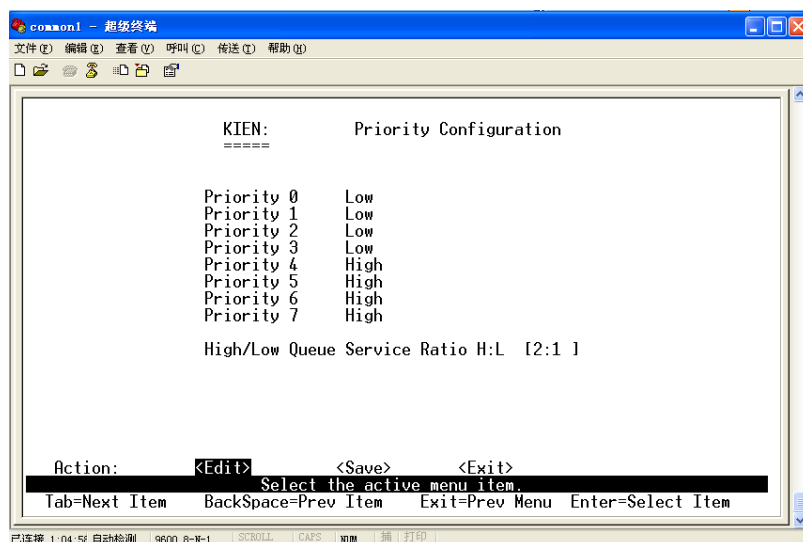


Figure2-28 Priority Configuration

In this page, there is priority 0-7 mapping to “High” or “Low queue”. “High/Low queue Service Ratio H:L” is for the setting of transmission ratio of high priority packets and low priority packets.

2. 2. 2. 6 MAC Address Configuration

“Switch Configuration” → “MAC Address configuration” → <Enter>.

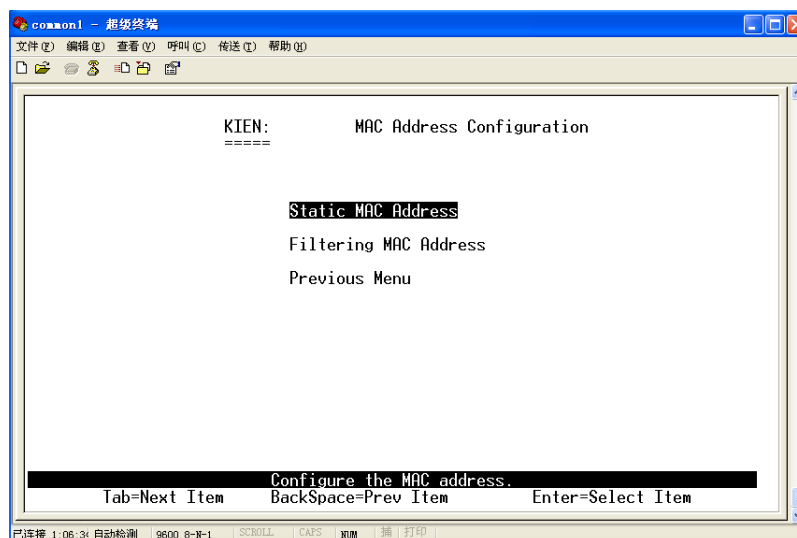


Figure2-29 MAC Address Configuration

1 . Static MAC Address Configuration

You can add, edit or delete static MAC address from this page.

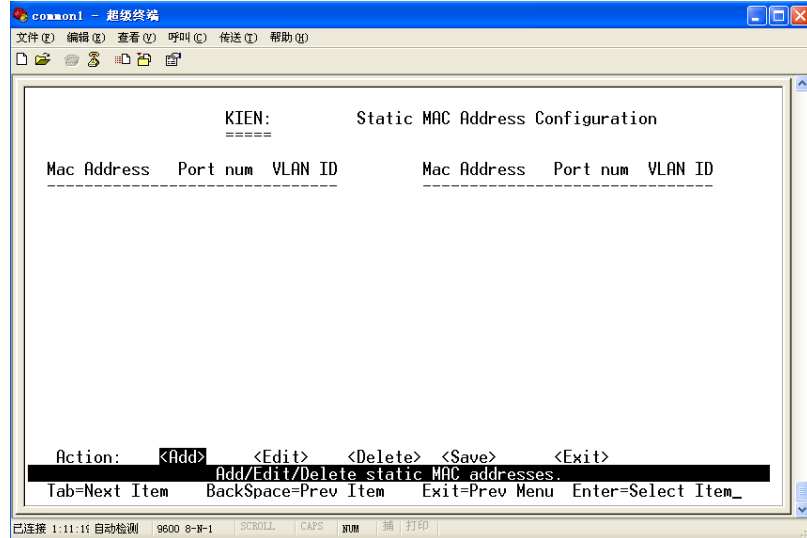


Figure2-30 Static MAC Address Configuration

When a static MAC address is added, it will be kept in the address table of the switch whether the physical device is connected with the switch or not, so that the switch do no need to study the address again after power supply cut-off or resetting.

1) Adding a static state MAC address

- “<Add> → <Edit>” →<Enter>, and then Add static MAC address.
- Type a MAC address, whose flow the switch’s port will always forward without considering the networking status.
- Type a port number.
- If the switch is set with tag-based (IEEE 802.1Q) VLAN, the static address must be related with the only VLAN. Type the VID related with MAC address.
- Press < Ctrl + A > to return to the main menu line and select <Save> and <Enter> to save all the configurations.

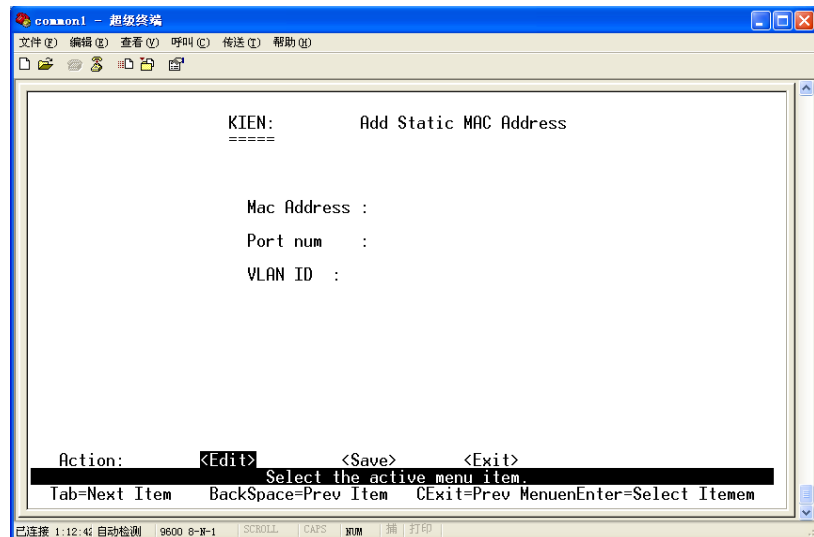


Figure2-31 Add Static MAC Address

2) Edit static MAC address

- a. Select <Edit> to change the static MAC address.
- b. Select the MAC address you want to change and press <Enter>.
- c. Select <Edit> to change the all items.
- d. Press < Ctrl + A > to return to the main menu line and select <Save> and <Enter> to save all the configurations.

3) Delete static MAC address

- a. Select <Delete> to delete static MAC address.
- b. Select the MAC address you want to delete and press <Enter>.
- c. <Save>→<Enter> to finish the operation.

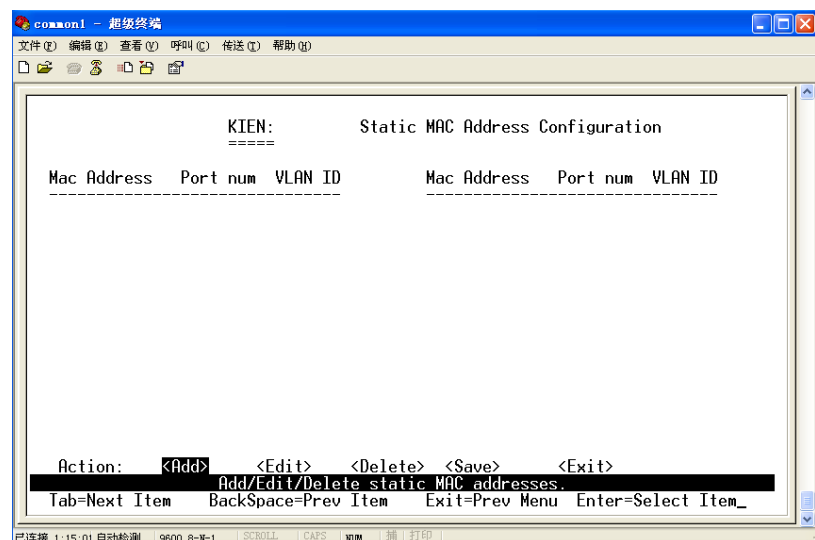


Figure2-32 Edit/Delete Static MAC Address

2 . Filtering MAC address configuration

MAC address filter allows the switch to drop the unwanted packets, which is based on destination address. You can add/edit/delete the filtering MAC address from this page.

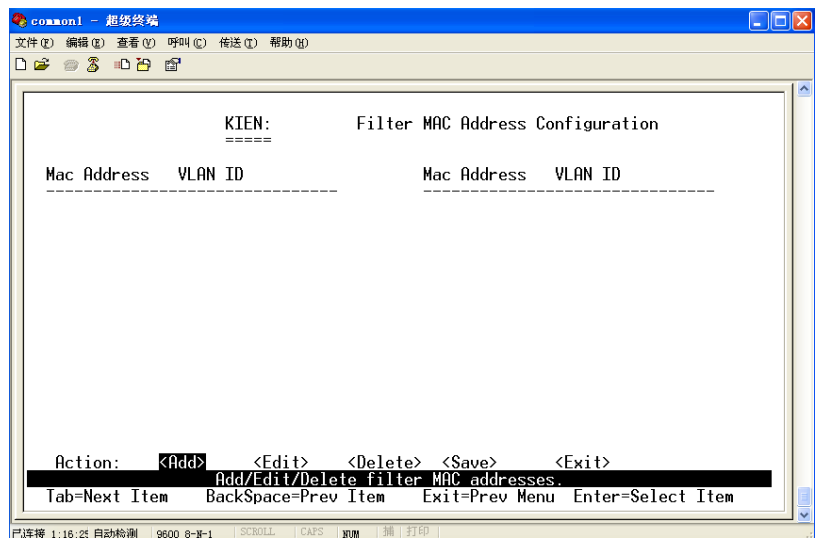


Figure2-33 Filter MAC Address configuration

- 1) Add
 - a. Select “<Add>→<Edit>” and <Enter> to add filtering MAC address.
 - b. Type a Filtering MAC address.
 - c. If the switch is set with tag-based (IEEE 802.1Q) VLAN, type the VID related with MAC address.
 - d. Press < Ctrl + A > to return to the main menu line and select <Save> and <Enter> to save all the configurations.

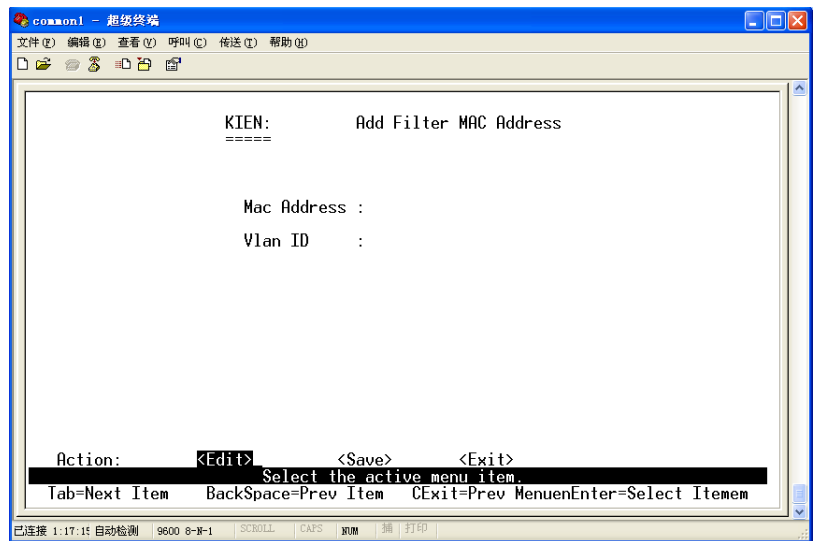


Figure2-34 Add Filter MAC Address

2) Edit

- a. Select <Edit> and <Enter> to edit the filtering MAC address.
- b. Select the filtering MAC address you want to edit and press <Enter>.
- c. Select <Edit> to change the all items.
- d. Press < Ctrl + A > to return to the main menu line and select <Save> and <Enter> to save all the configurations.

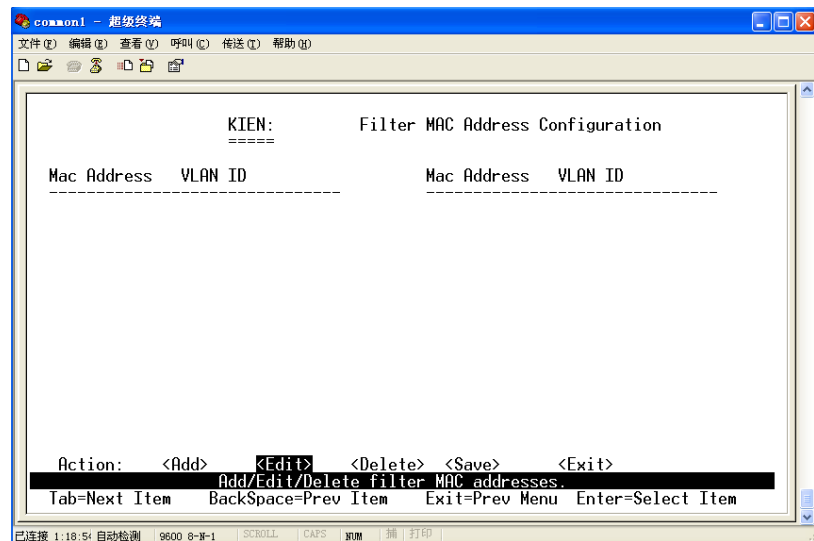


Figure2-35 Edit/Delete Filter MAC Address

3) Delete

- a. Select <Delete> to delete filtering MAC address.
- b. Select the filtering MAC address you want to delete and press <Enter>.
- c. <Save>→<Enter> to finish the operation.

2. 2. 2. 7 Misc Configuration

“Switch Configuration” → “Misc Configuration” →<Enter>. It's including “Port Security”、 “MAC Age Interval”、 “Broadcast Storm filtering”、 “Max Bridge Transmit delay bound” and “ Previous Menu”.

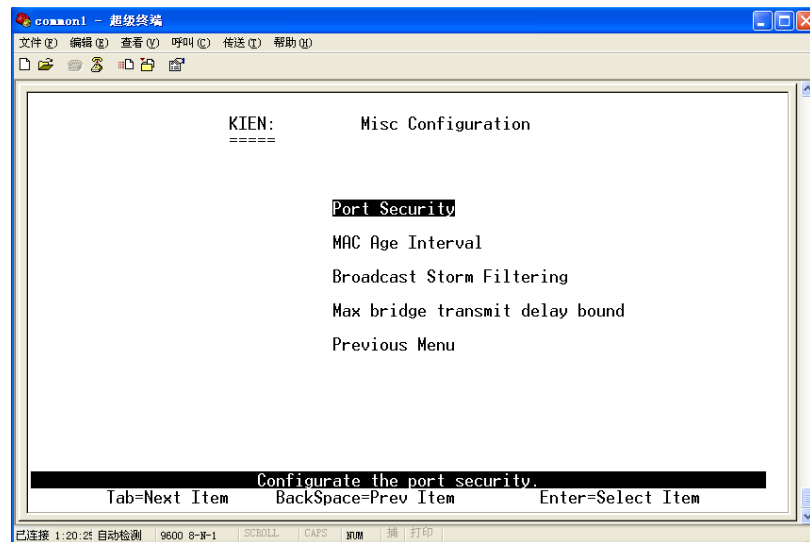


Figure2-36 Misc Configuration

1. Port security

A port whose security is enabled will be locked and not be allowed for address studying. For the incoming packets, only the packets with SMAC existing in the address can be forwarded. You can forbid the port to study any new address and define the MAC address list to use the secure port so as to prevent any illegal visit to the end devices.

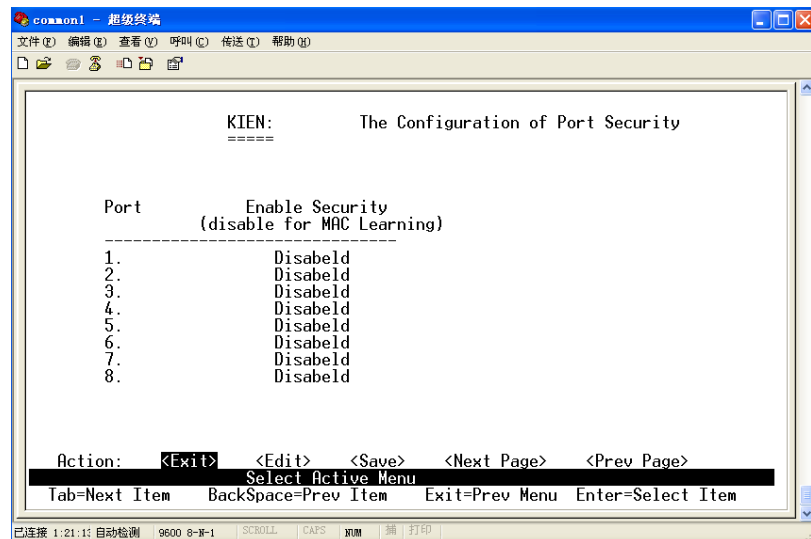


Figure2-37 Port Security

2. MAC Aging Interval

From this page, you can input inactive address and keep it in the switch's address table. The valid range is 300~765 second with 300 second as default.

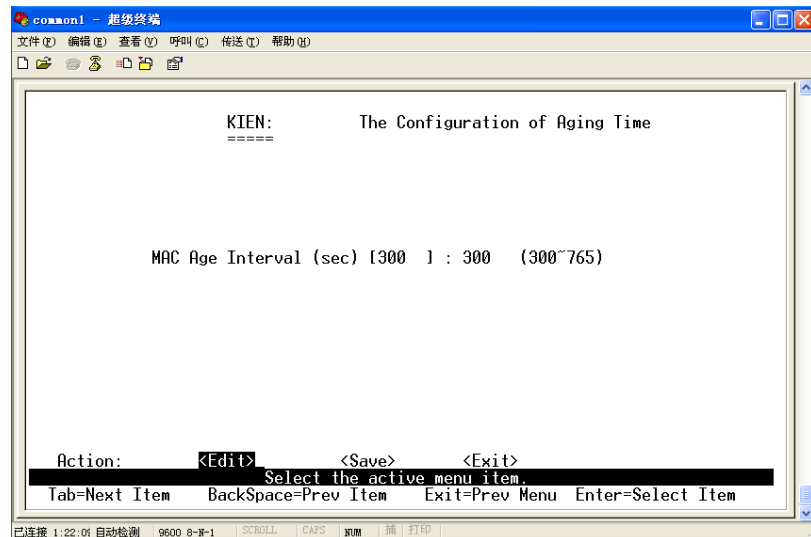


Figure2-38 MAC Aging Time

3. Broadcast Storm Filter

This page is for setting the broadcasting storm control. Select <Edit> and press <Enter> to configure the Broadcast Storm filtering mode. . <Space> is for you to select the threshold values. The valid values are 5%,10%,15%,20%,25% and closed.



Figure2-39 Broadcast Storm Filter

4. Max Bridge Transmit Delay Bound

The following table 2-7 shows all configurations of items.

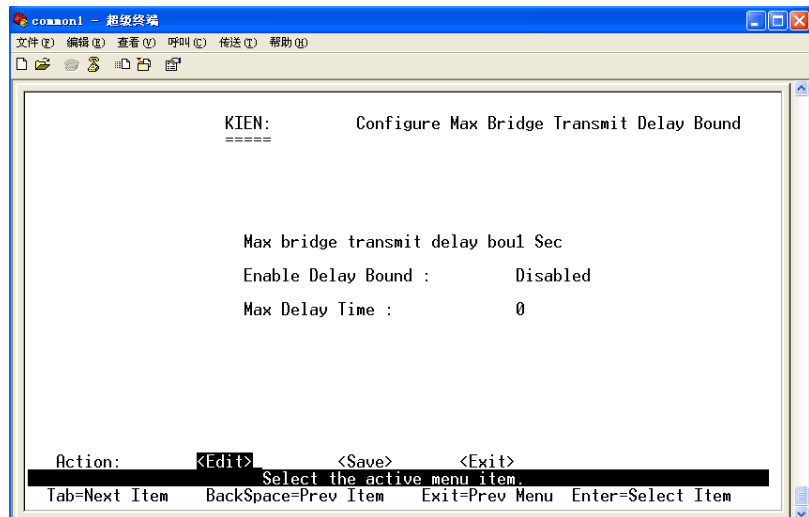


Figure2-40 Max Bridge Transmit Delay Bound

Table2-7 Meanings of Max Bridge Transmit Delay Bound

Item	Description
Max Bridge Transmit Delay Bound	To limit time for the packet to queue in the switch. If enabled, the overtime packets will be dropped. You can press <Space> to set the values. The valid value is 1sec, 2sec, and 4sec and closed, 1 sec is a default.
Enable Delay Bound	To limit time for the low priority packet to queue in the switch. If the time of low priority packet exceeds the maximum value, it will be transmitted.
Max Delay Time	The queuing time of the low priority packet. The max delay time is 255ms. The valid range is 0-255ms.

2. 2. 3 The Protocol Related Configuration

“The Protocol Related Configuration” → <Enter>. “The Protocol Related Configuration” is including “STP”、 “SNMP”、 “GVRP”、 “LACP”. Users select all item using by <Tab> or <Backspace>. “Main Menu” → <Enter> return to Main Menu.

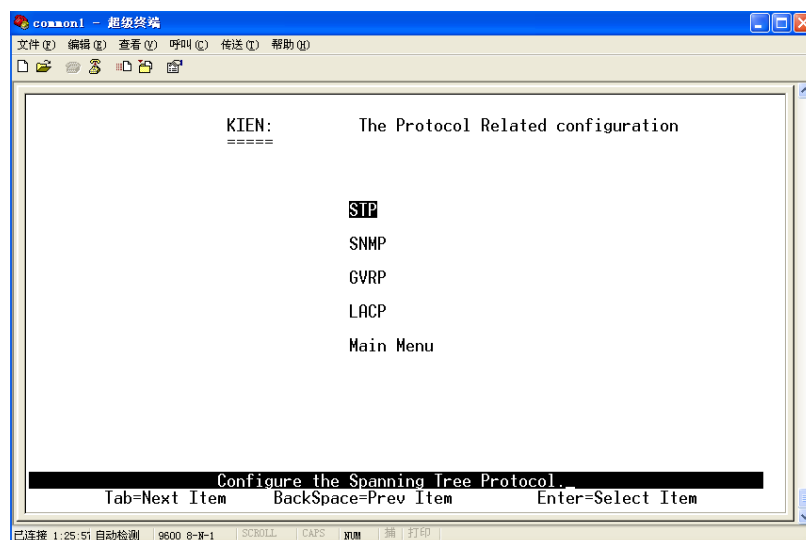


Figure2-41 the Protocol Related Configuration

2.2.3.1 STP

It contains three next menus: “STP Enable”、“System Configuration”、“Per port Configuration”.



Attention:

KIEN5000&KIEN6000 employ Kyland’s patented hardware redundancy technology. You are suggested not to use STP protocol unless you have a network mixing KIEN5000&KIEN6000 with other brand devices.

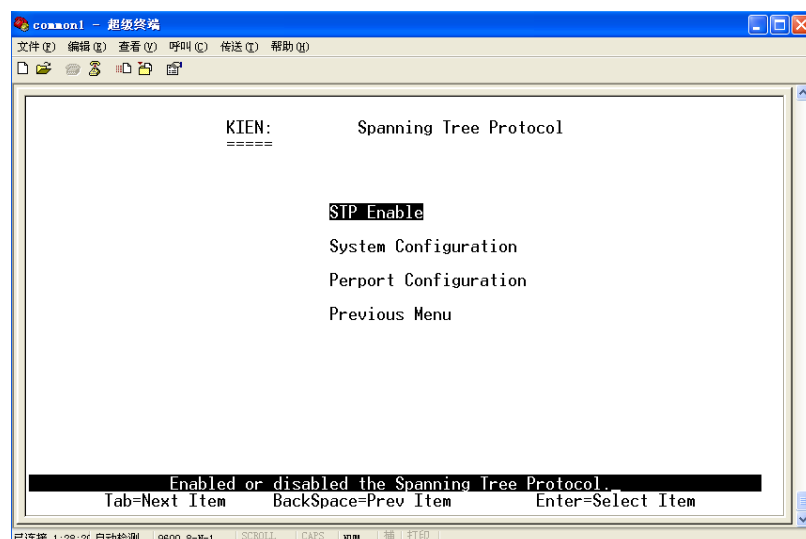


Figure2-42 STP

1. STP Status

This is for you to enable or disable Spanning Tree function. You can press <Space> to select Enable or Disable.

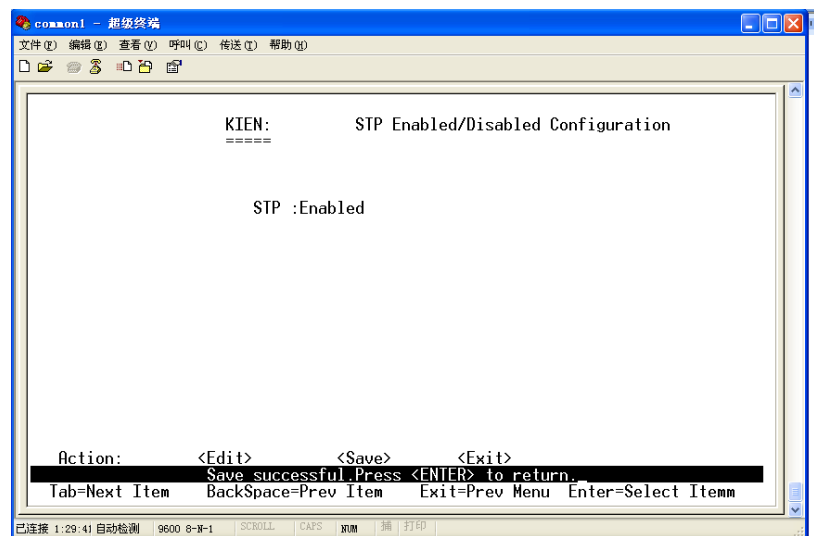


Figure2-43 STP Status

2. STP System Configuration

In the page below, the left side shows the information on the root bridge. You can set a new STP value on the right side. You can refer to the STP part in the Chapter four for the details on the parameters.

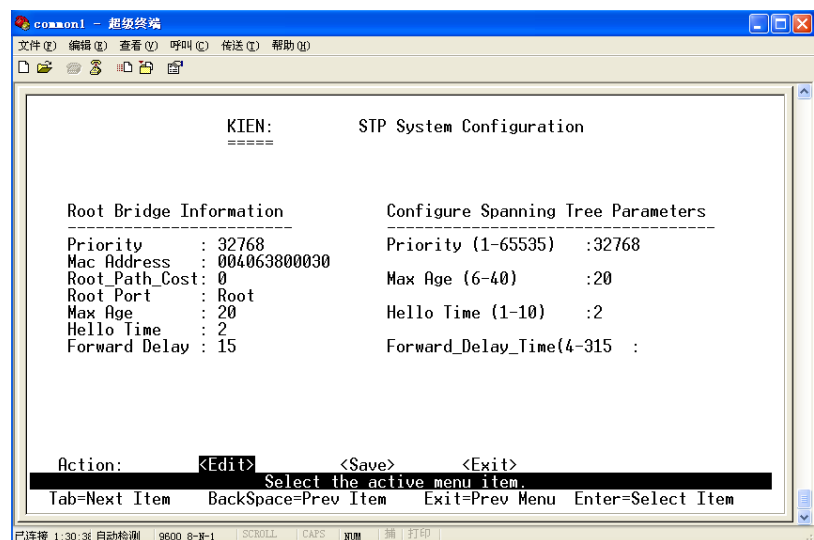


Figure2-44 STP System Configuration

3. STP Port Configuration

Table 2-8 shows particular description of per-port configuration.

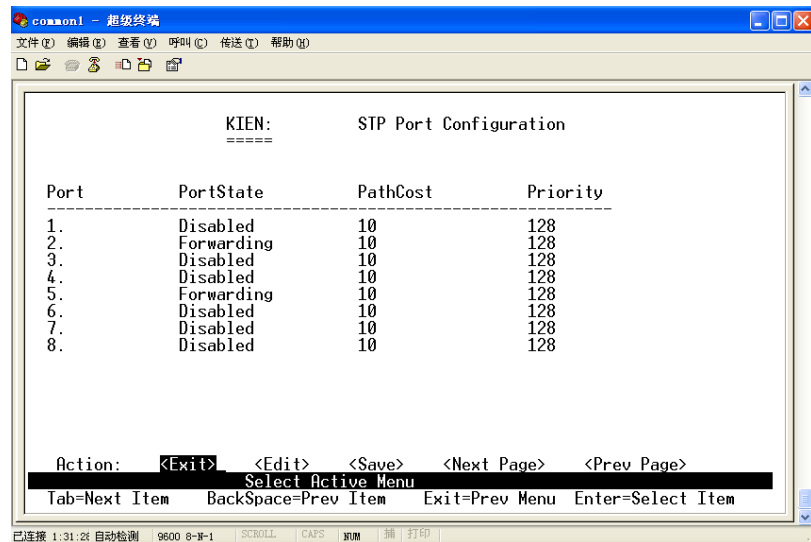


Figure2-45 STP Port Configuration

Table2-8 STP Port Configuration

Item	Description
Port State	Display the spanning tree status of each port in the switch.
Path Cost	The given path cost for the switch to decide which port is to forward. The smallest one will be the forwarding port, the range is 1~ 65535, the default value in IEEE 802.1D is 10Mb/s = 50-600; 100Mb/s = 10-60; 1000Mb/s = 3-10. To change the values, you need to re-set the switch.
Priority	By this setting, you can set the port as root, the value range is 0-255, 128 is the default. The smaller value, the higher priority. To change the value, you need to re-set the switch.

2. 2. 3. 2 SNMP Configuration

From this page, you can define the host PC as trap manager and input SNMP's community name. You can also define the name, location and contacts for the switch. This page is including three next menus: "System Options", "Community strings", "Trap Managers"

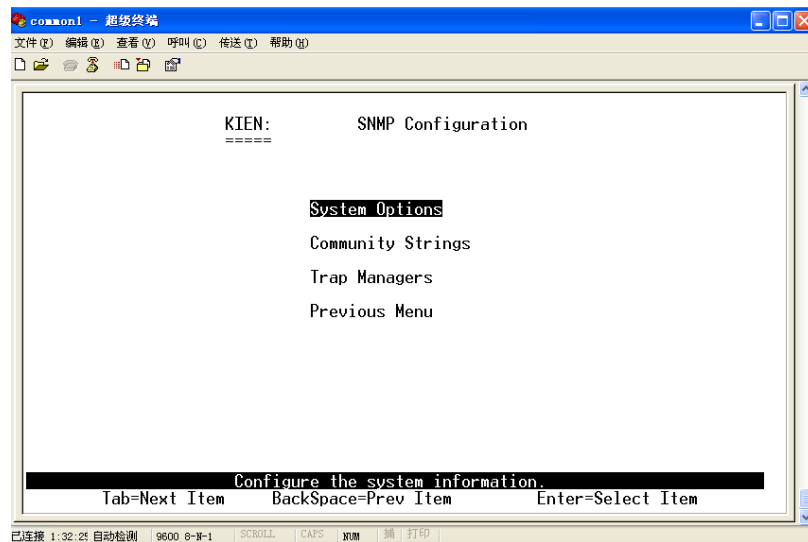


Figure2-46 SNMP Configuration

1 . System Options

Table2-9 shows description of system option.

Table2-9 System Options

Item	Description
System Name	Input switch name.
System Contact	Input system contact of switch
System Location	Input switch system location

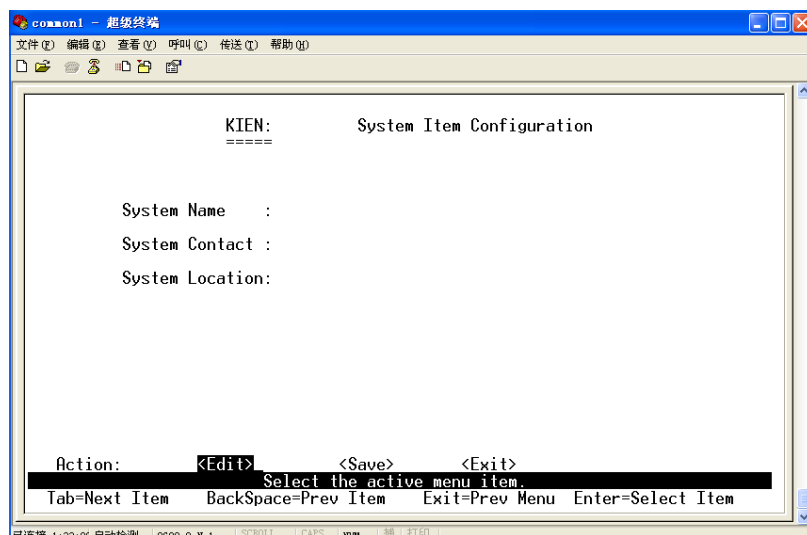


Figure2-47 SNMP System Item Configuration

2 . SNMP Community Configuration

You can configure SNMP Community Strings in this page.

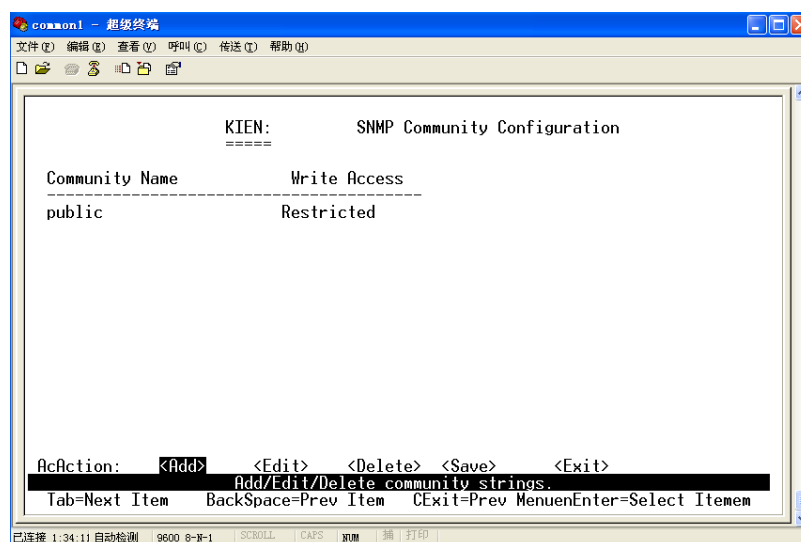


Figure2-48 SNMP Community Configuration

You can add or edit the strings by selecting <Add> or <Edit>, and <Edit> again. The details are as below Table2-10:

Table2-10 Add or Edit Strings

Item	Description
Community Name	Input the string name
Write Access	Restricted, read-only, enable the request with the name to display the MIB info.
	Unrestricted, read & write, enable the request with the name to display the MIB info and configure the MIB.

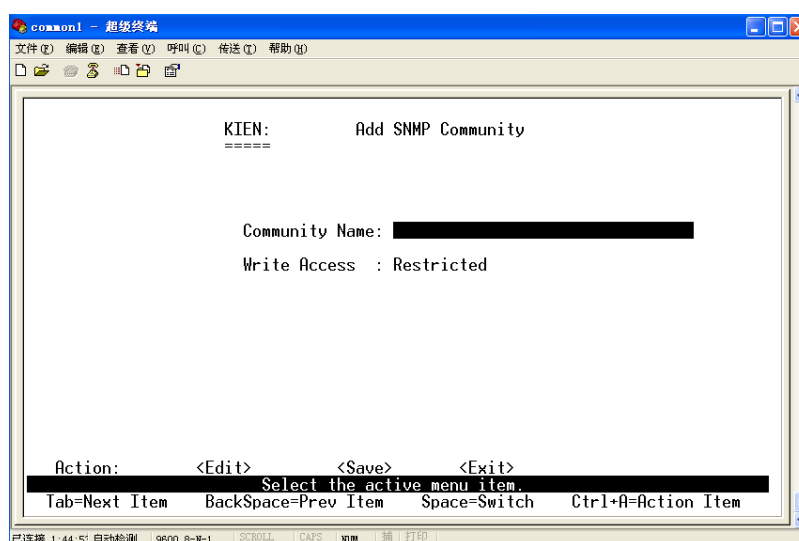


Figure2-49 Add or Edit SNMP Community

3. Trap Managers Configuration

Trap managers are the main station to receive the traps, which are the system warning generated by switch. If Trap Managers are not defined, the trap will not be sent. You can input IP address and group name to create a Trap Manager.

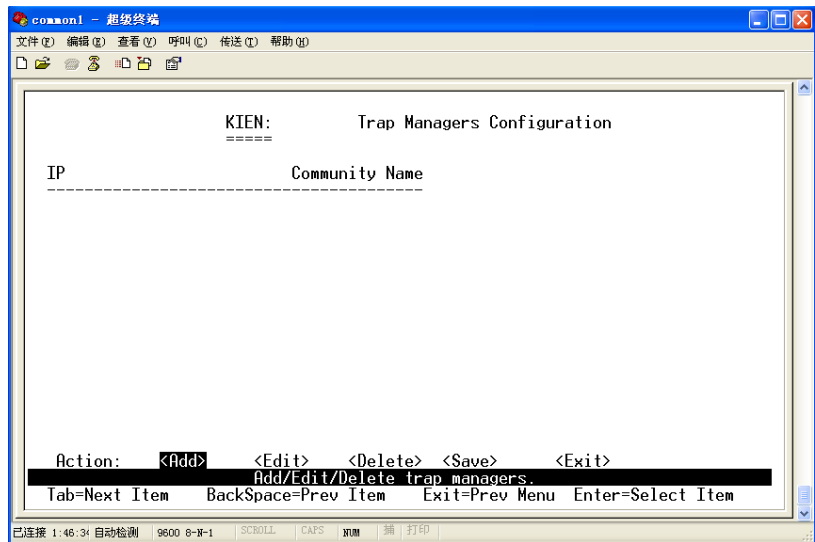


Figure2-50 SNMP Trap Managers Configuration

You can add or edit Trap managers.

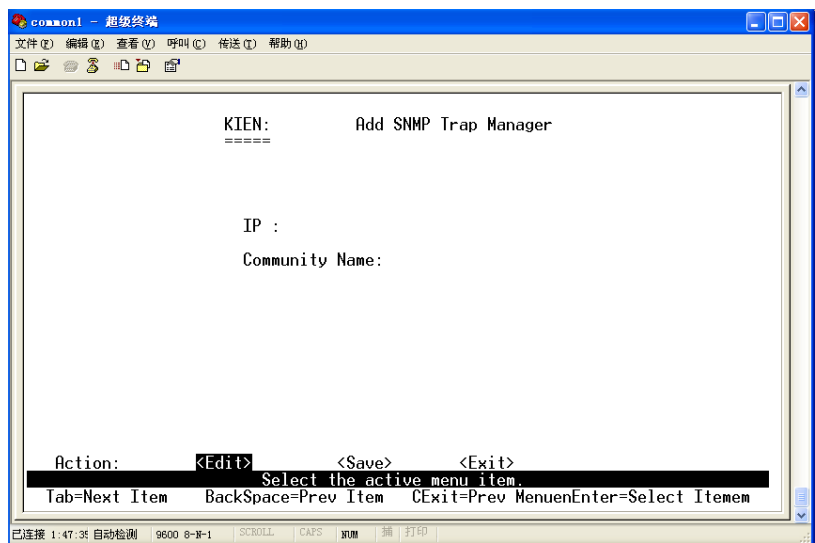


Figure2-51 Add or Edit SNMP Trap Manager

2. 2. 3. 3 GVRP

In this page, you can enable or disable GVRP （GARP VLAN Registration Protocol）. Table 4-5 shows description of GVRP.

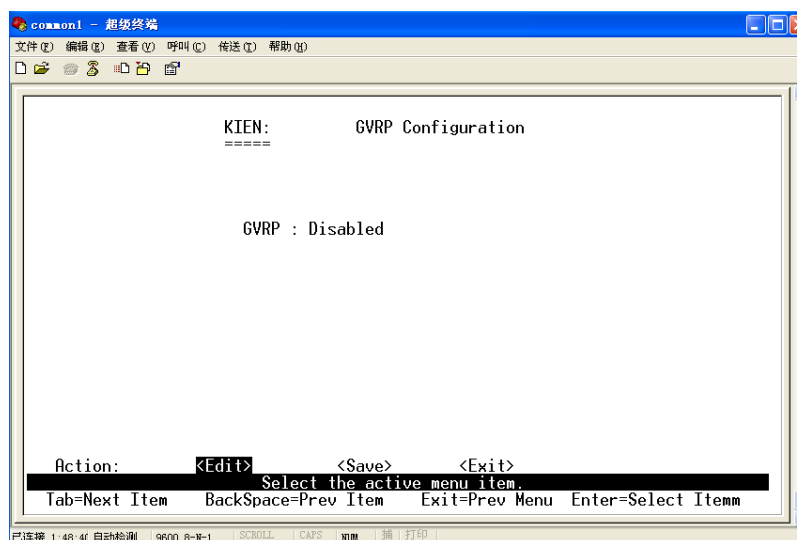


Figure2-52 GVRP Configuration

2.2.3.4 LACP

There are three options in this page. “Aggregator Setting”、“State Activity”、“LACP STATUS” shown as following.



Figure2-53 LACP

1 . Aggregator Setting

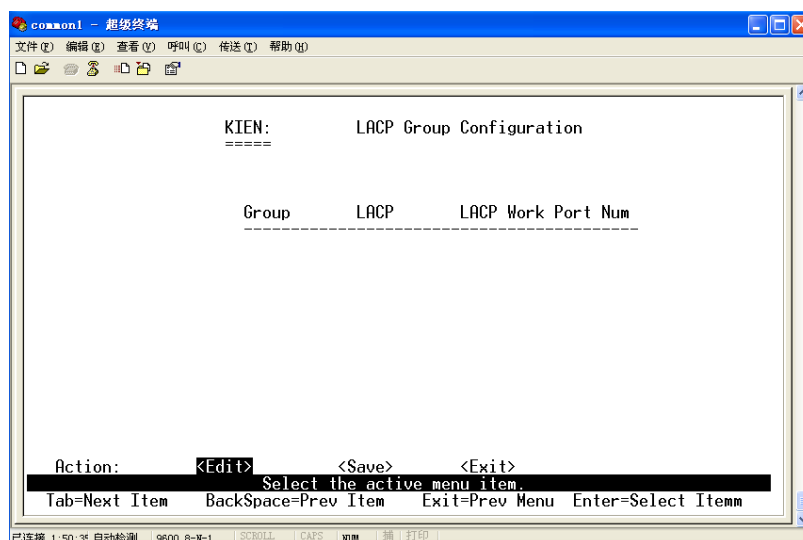


Figure2-54 LACP Group Configuration

Table2-11 shows description of all items.



Attention:

Before configuring LACP, you must configure aggregate group in "Port/Trunk Configuration" page

Table2-11 LACP

Item	Description
Group	Shows aggregation group ID.
LACP	You can convert LACP between enable and disable by pressing <Space>. If enabled, the group is LACP static trunking. If disabled, the group is local static trunking.
LACP Work Port Number	The maximum quantity of ports aggregated simultaneously. For LACP static trunking group, the rest ports will be backup and aggregate for the failure of working ports. For local static trunking group, the number must be comply with the port quantity.

2 . State Activity

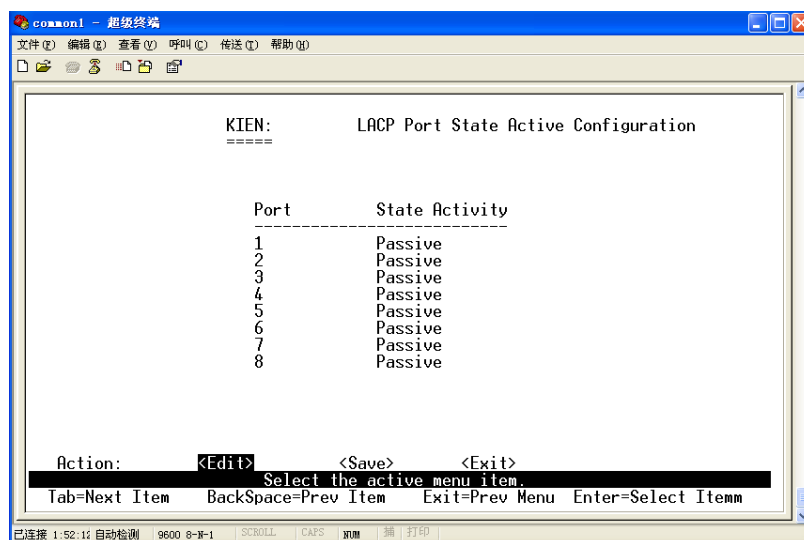


Figure2-55 LACP Port State Active Configuration

After selecting <Edit> and <Enter>, you can edit each port's properties by pressing <Space> key. The passive port will not send automatically LACP protocol packets; only after receiving the LACP packet can it respond. Active port will send the LACP protocol automatically.

3 . LACP State

You can check the information in this page if you have set a trunking group.

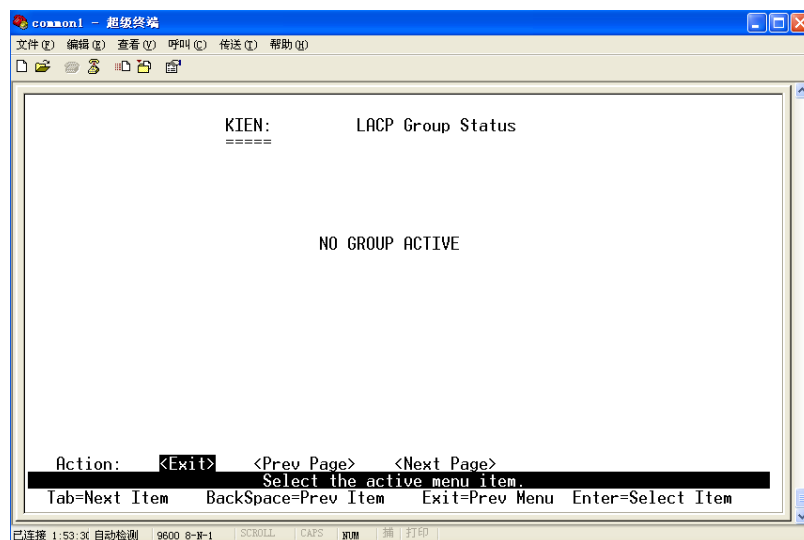


Figure2-56 LACP Group Status

2. 2. 4 Restart Switch

“Restart Switch” → <Enter>.

“Restart Switch” including “Default” and “Restart”. You can select items by using <Tab> or <Backspace>. When select “Previous Menu” go back to Main Menu.

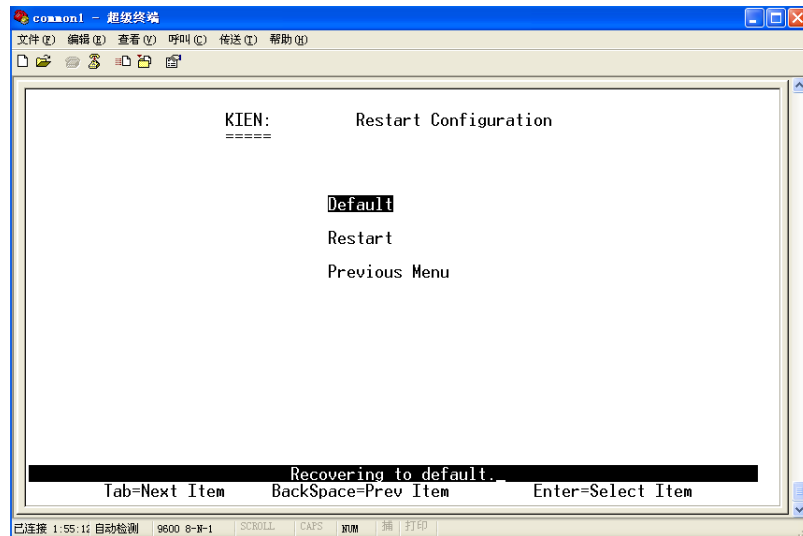


Figure2-57 Restart Switch

When you select “Default”, the switch is set as the default settings, which can be referred in Table4-11. You can restart the switch by select “Restart”.

2.2.5 Command Line

This item can switch from menu to command mode. All about commands please see Chapter Three.

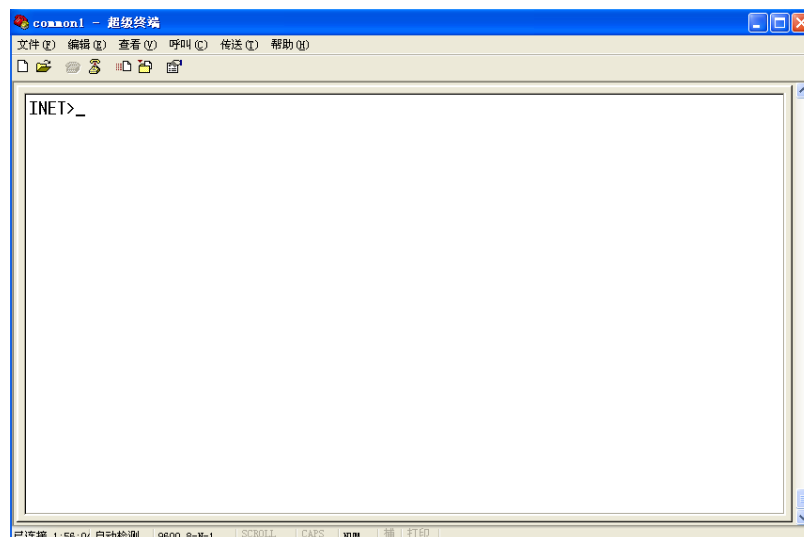


Figure2-58 Command Line

2. 3 1K Xmodem software

KIEN5000 and KIEN6000 Industrial Ethernet Switch support to upgrade software by using 1K Xmodem protocol in console mode. 1K Xmodem work only in 57600bps mode, so only when you set 57600bps in console mode, can you download software.

You can update software in the two situations as below:

- 1 . Press “shift + x” within 5 seconds after it is powered in the console management interface.
- 2 . If the system find the failure of software checking in the boot period, it will get in automatically “1K Xmodem Receiving Model”.

When the system is in “1K Xmodem receiving mode”, you can change bit rate into 57600bps and select “Transfer” → “Send File”, then input the new position of the document to be updated, select “1K Xmodem” and send to start updating the software.

After finish the updating, you need to restart the switch while make sure the bit rate is set as 9600bps.

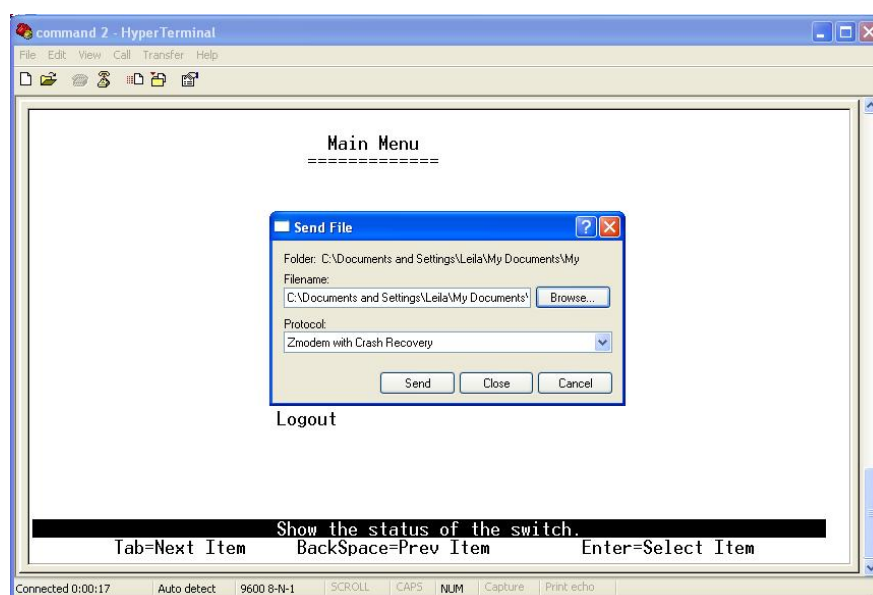


Figure2-59 1K Xmodem Update Software

Chapter Three Command of Console Port

3. 1 System Configuration

Command	Description
show IP	Show IP address, sub mask and gate way
configure IP	Configure IP address of switch
configure subnet	Configure sub mask address of switch
configure gateway	Configure gate way address of switch
show Mac	Show MAC address of switch
show version	Show version of software
show console	Show information of console
configure default	Back to default switch
reboot	Restart switch
quit	Back to main Menu

3. 2 Switch Configuration——Advanced

Command	Description
Age-out Time	
Enable fdbage	Enabled MAC address auto aging time
Disable fdbage	Disabled MAC address auto aging time
Config fdbage<number>	Configure MAC address auto aging time (300~765 second).
Show fdbage	Show aging time of switch.
Broadcast Storm Filter	
Enable bsf[5 10 15 20 25]	Enabled or configure Broadcast Storm filtering. For example: enable bsf 10
Disable bsf	Disable Broadcast Storm filtering
Show bsf	Show configuration of Broadcast Storm filtering
Priority Queue Service	
Config qos[fcfs/wrr/strict]<hw:1~7><lw:1~7>	Configure PRI service: Fcfs: first come first service Wrr: Weight Round-Robin Strict: all high before low <hw>: High level priority, valid values are from

	1-7, only valid in WRR mode. Ex: Config qos fcfs Config qos wrr 5 1
Enable qdlyb<1~255>	Enable the low queue delay bound function and configure the delay bound time threshold value. The valid value is 1-255ms. Ex: enable qdlyb 200.
Disable qdlyb	Disable queue delay bound function.
Show qos	Show Qos configuration
Config qospolicy<high level list>	Configure QoS. PRI 0~7 mapped to high or low queue.. <high level list>: belongs to high PRI. (0~7). Ex: config qospolicy 0~3

3. 3 Port Control

Command	Description
Show portstatus <portlist>	Show status of per or multi port. <portlist>: port number. Ex: show portstatus 1-10 show portstatus 1,3,5
Show statistics <portlist>	Show status of per or multi port. Ex: show statistics 1-10 show statistics 1,3,5
Config ports <portlist> state [off/on]	Change configuration of one group port. <portlist>: port number. state off: disabled the port state on: enabled the port Ex: config ports 1-5 state off
Config ports <portlist> auto [off/on]	Enabled or disabled automatism of port. <portlist>: port number. auto off: disabled auto auto on: enabled auto Ex: config ports 1-5 auto off
Config ports <portlist> ability [10full 10half 100full 100half]	Change speed of port and configure duplex mode. <portlist>: port number. Ex: config ports 6,7 ability 10full

		<groupid>: LACP static trunking group ID. <number>:The quantity of ports that can be aggregated simultaneously.
enable	lacp	Change the native trunking mode into LACP mode.
<groupid:1~4>		
disable	lacp	Change the LACP mode into native trunking mode.
<groupid:1~4>		
Add trkgrp <1~4> ports		Add trunking port.
<portlist:1~8>		
del trkprrt <portlist:1~8>		Delete trunking port.
trkgrp <1~4>		

3. 5 Filtering Data

Command	Description
IGMP snooping	
enable igmp	Enabled IGMP filtering
disable igmp	Disabled IGMP filtering.
show igmpstate	Show configuration of IGMP (enabled / disabled).
Port Security	
enable security <portlist>	<portlist>:port number Ex: enable security 1,3 For port security, enable MAC address study in one or multiple ports.
disable security <portlist>	For port security, disable MAC address study in one or multiple ports. <portlist>: port number. Ex: disable security 1,3
Static MAC addresses	
add fdb <p> mac <mac_address> vid <number> port <number>	Establish static MAC address. Ex: add fdb p mac 001234567890 vid 1 port 1
delete fdb <p> mac <mac_address> vid <number> port <number>	Delete static MAC address. Ex: delete fdb p mac 001234567890 vid 1 port 1
clear fdb p	Clear all static MAC address.
show fdb p	Show all static MAC address.

MAC Filtering	
add fdb mac <mac_address> vid <number>	Configure the MAC address whose info is unwanted. The filtered packets are based on destination address. Ex: add fdb b mac 001234567890 vid 1 port 1
delete fdb mac <mac_address> vid <number>	Delete switch filtering MAC address. Ex: delete fdb b mac 001234567890 vid 1 port 1
clear fdb b	Clear all switch filtering MAC address.
show fdb b	Show all switch filtering MAC address.

3. 6 VLAN

Command	Description
add vlan <name> vid <number 1> protocol <number 2> ports <portlist> [tag/untag]	Create VLAN group. <name>:Name the VLAN. The valid string is 1-15. <number 1>: Assign one number as the VLAN ID. Available in 1~4094. <number 2>: Assign a user-defining protocol. The valid range is 0-18. About protocol please see Table A. <portlist>: port number. Ex: add vlan v1 vid 2 protocol 0 ports 1,2 tag
config vlan <name> protocol <number>	Configure protocol in existent VLAN. <name>: existent VLAN name. Ex: config vlan v1 protocol 5
config vlan <name> addport <portlist> [tag/untag]	Add per or multi port in VLAN group. User can point to port as tagged or untagged. Ex: config vlan v1 addport 3,4 tag
config vlan <name> delport <portlist>	Delete per or multi port in VLAN. Ex: config vlan v1 delport 3,4
Config vlan <name> tag <portlist>	Configure tagged port in VLAN. Ex: config vlan v1 tag 1
config vlan <name> untag <portlist>	Configure untagged port in VLAN. Ex: config vlan v1 untag 2
delete vlan <name>	Delete VLAN via name. Ex: del vlan v1

delete vlan vid <1~4094>	Delete VID via name Ex: del vlan vid 2
show vlantbl <name>	Show VLAN information.
show vlantblindex	Show all VLAN name of switch.
enable vlan gvrp	VLAN configure as "802.1Q with GVRP" mode.
disable vlan gvrp	VLAN configure as "802.1Q without GVRP" mode.
show vlanstate	Show VLAN status.
show prtcl vlantbl	Show VLAN protocol.
config vlan pvid <1~4094> ports <portlist>	Configure PVID of per- port.

3. 7 Spanning Tree

Command	Description
enable stp	Enabled spanning tree protocol.
disable stp	Disabled spanning tree protocol.
config stp hellotime <number>	Configure the time of transmitting spanning tree protocol info. <number>: 1~10 is valid.
config stp maxage <number>	The time bridge need to wait before trying to set again when the bridge does not receive the spanning tree news. <number>: 6 ~ 4 0 is valid.
config stp fwdly <number>	The time it takes to convert from spanning tree study and monitor status to forward status. <number>: 4 ~ 3 0 is valid.
config stp priority <number>	The value to recognize root bridge. The bridge of smallest value will have the highest priority and be selected as root. To change this value, you need to restart the switch. <number>: 1 ~ 6 5 5 3 5 is valid.
show stp portstatus	Show spanning tree status of per-port.
show stpstate	Show STP function (Enabled / Disabled).
show stp info	Show configuration of STP.

show stp rootbridge	Show STP information of Root Bridge.
---------------------	--------------------------------------

3.8 Sniffer

Command	Description
enable sniffer <portid> rx <portlist> tx <portlist>	Enabled and configure port sniffer. <portid>: configure port(1~10). <portlist>:Configure the port whose rx or tx flow the user want to monitor. 1-10 is valid. Ex: enable sniffer 10 rx 1-5 tx 4-9 or enable sniffer 10 rx 1-5 tx 0
disable sniffer	Disabled port sniffer.
show sniffer	Show configuration of port sniffer.

3.9 Table A

Serial Number of Protocol	Type of Protocol
0	None
1	IP
2	ARP
3	Appletalk
4	AppletalkAAPP
5	Novell IPX
6	Banyan VINES
7	DECnet MOP
8	DECnet DPR
9	DECnet LAT
10	DECnet LAVC
11	IBM SNA
12	X.75 Internet
13	X.25 Layer3
14	NetBIOS
15	IOS Network Layer PDU
16	Novell IPX(raw Ethernet)
17	Spanning Tree Protocol BPDU
18	Null SAP

Chapter Four WEB Management

4. 1 WEB Network Management

WEB browser supports an easy way to watch and manage in KIEN5000 and KIEN6000 Industrial Ethernet Switch. User can choose any browser including IE, Netscape and any others.

When logging in, user can refer to the product mark. To confirm or change IP address, user can login WEB Management. Example as follows:

MAC address: 000060006000

IP address: 192.168.0.2

Subnet Mask: 255.255.255.0

Gateway: 192.168.0.1



Attention:

If Web browser login console, firstly the switch needs be connected to network from RJ-45 Ethernet port or to PC by straight-through cable.

KIEN5000 and KIEN6000 Industrial Ethernet Switch Default IP Address:192.168.0.2

KIEN5000 and KIEN6000 Industrial Ethernet Switch Default User Name: admin,
Password:123.

User can login WEB Management step by step.

- 1 . Firstly, run IE or other Web browser, type IP address of KIEN5000 or KIEN6000, and then press [Enter].The figure as follows:



Figure4-1 Star-up WEB Network Management

- 2 . If password setting already, and then login user name and password (same with console) .



Figure4-2 Login WEB Network Management

WEB Network Management homepage as follows :

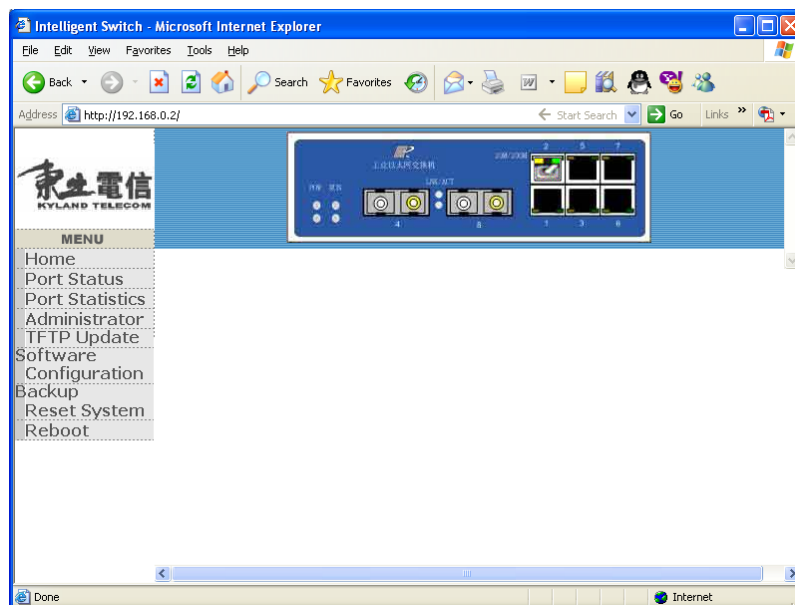


Figure4-3 WEB Network Management Homepage

4. 2 Port Status

“Port Status” shows status of port, the figure as follows:

The following information provides a view of the current status of the unit.

Port Num	State		Link	Auto		Speed Status		Duplex Status		Flow Control	
	Config	Actual		Config	Actual	Config	Actual	Config	Actual	Config	Actual
1	On	Off	Down	Auto	Auto	100	100	Full	Full	On	On
2	On	On	Up	Auto	Auto	100	100	Full	Full	On	On
3	On	Off	Down	Auto	Auto	100	100	Full	Full	On	On
4	On	Off	Down	Close	Close	100	100	Full	Full	On	On
5	On	Off	Down	Auto	Auto	100	100	Full	Full	On	On
6	On	Off	Down	Auto	Auto	100	100	Full	Full	On	On
7	On	Off	Down	Auto	Auto	100	100	Full	Full	On	On
8	On	Off	Down	Close	Close	100	100	Full	Full	On	On

Figure4-4 Port Status

Table4-1 Port Status

Entry	Description
State	Two kind of state: On or Off. “Down”act as “Close”.
Link	Disconnection act as “Down”, Connect act as “up”.
Auto	Automatism mode.
Speed Status	Shows 1000Mbps,100Mbps and 10Mbps; Port 1 to 8 is 10/100Mbps, Port 9 to 10 is 10/100/1000Mbps.
Duplex Status	Shows Full/half Duplex status mode.
Flow Control	Shows Activated or Inactivated mode.
Configure	Shows status of user configure.
Actual	Shows result.

4. 3 Port Statistics

“Port Statistics” shows statistics of port as follows:

The following information provides a view of the current status of the unit.

Port	State	Link	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt	TxAbort	Collision	DropPkt
1	Off	Down	0	0	0	0	0	0	0
2	On	Up	101929	0	256871	0	0	0	9502
3	Off	Down	0	0	0	0	0	0	0
4	Off	Down	0	0	0	0	0	0	0
5	Off	Down	0	0	0	0	0	0	0
6	Off	Down	0	0	0	0	0	0	0
7	Off	Down	0	0	0	0	0	0	0
8	Off	Down	0	0	0	0	0	0	0

Figure4-5 Port Statistics

4. 4 Administrator

Including: IP Address、Configuration、Console Information、Port Control、Aggregator、Filter、VLAN Configure、Spanning Tree、Port mirror、SNMP、Security Management as following figure:

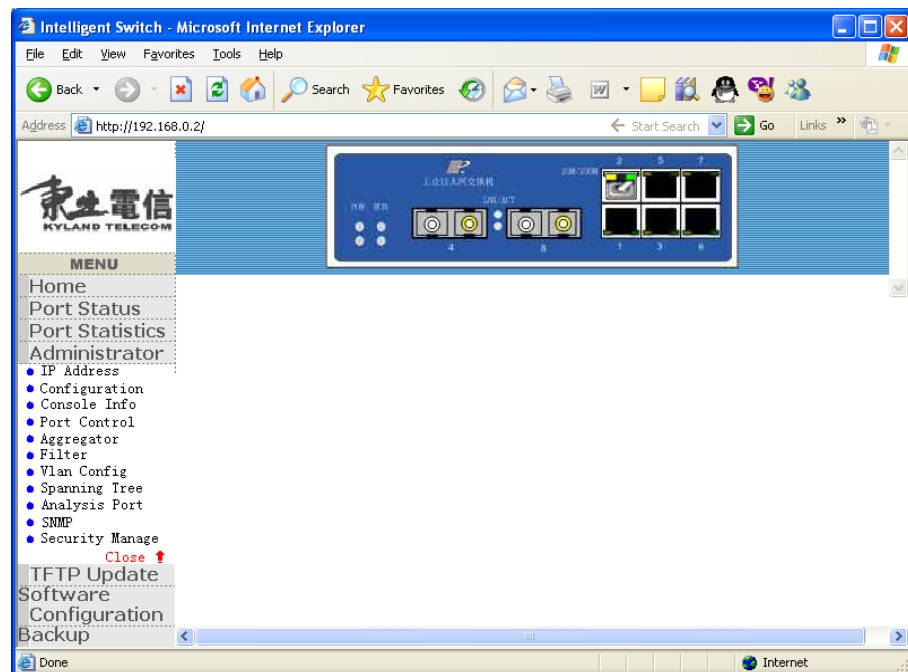


Figure4-6 Administrator

4. 4. 1 IP Address

Click “Administrator” → ”IP Address”, shows IP address、subnet mask、Gateway address. User can configure IP address, type new value, Click “Apply”, it will be done after restart.

IP Address	192.168.0.2
Subnet_Mask	255.255.255.0
Gateway	192.168.0.1

Figure4-7 IP Address

4. 4. 2 Configuration

4. 4. 2. 1 Basic

Click “Administrator” → “Configuration”, shows basic information.

Table 4-2 Configurations

Item	Description
Description	Shows name of device.
MAC address	unique hardware address by manufacturer (default) .
Version	Shows version of switch.
Hardware	Shows hardware version.
Default configure value version	Shows default version for memory writing

Basic	Advanced
Description	KIEN Switch
MAC Address	000061006039
Version	v01.01
Hardware	A03.00
Default config value version	v09.17

Figure4-8 Configuration

4. 4. 2. 2 Advanced

Click “Advanced”, including other setting、Priority Queue Service、Protocol Enable Setting etc..

Basic
Advanced

Enter the settings, then click Submit to apply the changes on this page.

☒ MAC Table Address Entry Age-Out Time: seconds

Max bridge transmit delay bound control:

Broadcast Storm Filter Mode:

Priority Queue Service:

☐ First Come First Served

☐ All High before Low

☒ WRR

High weight: Low weight:

☐ Enable Delay Bound

Max Delay Time: ms

QoS Policy: High Priority Levels

☐ Level0 ☐ Level1 ☐ Level2 ☐ Level3

☒ Level4 ☒ Level5 ☒ Level6 ☒ Level7

Protocol Enable Setting:

☐

Figure4-9 Advanced

1 . Other Setting

Table4-3 Other Setting

Entry	Description
MAC Address Age-out Time	The time for inactive MAC address in table, from 300 to 765 second. Default is 300 second.
Max bridge transmit delay bound control	virtual value is 1 second, 2 second, 4 second and close. Default is 1 second.
Broadcast storm filter mode	The value is the percentage the broadcast flow accounts for in the bandwidth of port. Broadcast storm will be activated when flow of broadcast exceeds active value too much. Active value is 5%, 10%, 15%, 20%, 25% and close.

2 . Priority Queue Service

Table4-4 Priority Queue Service

Entry	Description
First come first	Sequence of packets sending depends on coming.

served	
All high before Low	All high priority sent before low priority sent.
WRR	For property setting of packets in the priority queue, which means the quantity of high priority packets sent before low priority ones. Ex: High weight 5, Low weight 1 means 5 high priority packets are sent out before 1 low priority packet is.
Enable Delay Bound	To limit the queuing time of low priority packet. Default delay is 255ms max. Once the time exceeds the limit, the packets will be sent out. The value range is 1~255ms. Notes: Before set Enable Delay Bound, make sure “Max bridge transmits delay bound control” is enabled.
Qos policy: high priority level	0~ 7 levels mirrors high or low queue.

3 . Protocol Enable Service

Table4-5 Protocol Enable Service

Entry		Description
Enable STP Protocol		Default closed STP. Recommended
Enable IGMP Protocol		Enable IGMP.
VLAN	No VLAN	VLAN inactivated
	Port-based	Port-based VLAN
	802.1Q without GVRP	Support 802.1Q , but GVRP without dynamic VLAN.
	802.1Q with GVRP	Support 802.1Q and GVRP with dynamic VLAN.
GVRP (GARP[General Attribution Registered Protocol] VLAN registered protocol)		GVRP allows the automatic configuration between switch and nodes. For a switch connected to GVRP enabled device, its defined VLAN's VID can send GVRP request and it will automatically add the device to the VLAN.

4. 4. 3 Console Information

Click “Administrator” → “CONSOLE Information”, shows the basic info about serial port of PC CONSOLE as followed.

Baudrate	9600
Data Bits	8
Parity Check	None
Stop Bits	1
Flow Control	None

Help

Figure4-10 Console Information

4. 4. 4 Port Control

Click “Administrator” → “Port control” Any change can de made to the port status in this page. The figure as follows:

Port	State	Auto Negotiation	Speed	Duplex	Flow Control
1					
2	Enable	Enable	100	Full	Enable
3					
4					

Apply

The following information provides a view of the current status of the unit.

Port Num	State		Link	Auto		Speed Status		Duplex Status		Flow Control	
	Config	Actual		Config	Actual	Config	Actual	Config	Actual	Config	Actual
1	On	Off	Down	Auto	Auto	100	100	Full	Full	On	On
2	On	On	Up	Auto	Auto	100	100	Full	Full	On	On
3	On	Off	Down	Auto	Auto	100	100	Full	Full	On	On
4	On	Off	Down	Close	Close	100	100	Full	Full	On	On
5	On	Off	Down	Auto	Auto	100	100	Full	Full	On	On
6	On	Off	Down	Auto	Auto	100	100	Full	Full	On	On
7	On	Off	Down	Auto	Auto	100	100	Full	Full	On	On
8	On	Off	Down	Close	Close	100	100	Full	Full	On	On

Figure4-11 Port Control



Attention:

When user setting “Auto-negotiation” or ”Duplex Status”, ”Speed Status” must mach the real device settings.

4. 4. 5 Aggregator

Click “Administrator” → “Aggregator”. Aggregator control protocol offers a standard way for the equivalent systems to exchange information in one link. In this way, the aggregator control of equivalent systems can know to which group its link belongs and move its link to the right group, in addition, the transmitting and receiving function will be opened in a sequence way. Link aggregator can aggregate multiple sequent ports into a trunk, which can expand the bandwidth of networking device. Full duplex is required for a link aggregator control protocol. For more details, please refer to IEEE 802.3ad.

4. 4. 5. 1 Aggregator Setting

Aggregator setting shows as follows:

Aggregator Setting

Aggregator information

State Activity

System Priority

1

Group ID	Group1	<< Get
LACP	Disable	
Work Ports	0	
	<< Add << Remove >>	port1 port2 port3 port4 port5 port6 port7 port8

Apply

Delete

Help

Figure4-12 Aggregator

The meaning of each item as follows:

Table4-6 Aggregator settings

Item	Description
System Priority	For marking the active LACP value. The switch with the lowest value has the highest priority and is selected as active

	LACP.
Group ID	You can set up link aggregator among two or more ports. Choose “Group ID” and Click “Get”.
LACP	If enabled, the group is in LACP static trunking. If disabled, the group is in local static trunking. All ports supports LACP dynamic trunking grouping. If all connected devices support LACP, the PACP dynamic trunking will be formed automatically. If LACP enabled, LACP can be set into positive/passive status in each port. Notes: When you configure the trunking, make sure the STPP is opened; otherwise, a redundant link is formed in the ring network and cause network to break down.
Work Ports	The maximum ports that can be aggregated simultaneously. If in a LACP trunking group, the additional ports is stand-by and aggregated when work port is not valid. If in a local static trunking group, the setting must be consistent with the ports of group.
Add	To add port of Trunking.

4. 4. 5. 2 Aggregator Information

Click “Aggregator Information”, you can see the info below when you set LACP Aggregator as follows.

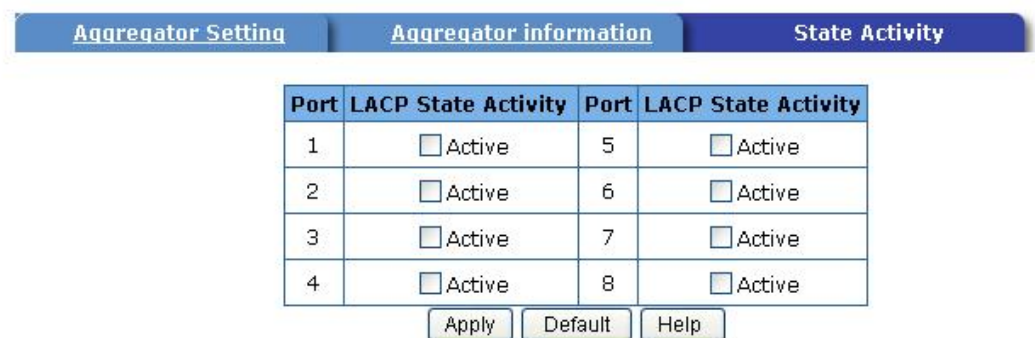


Figure4-13 Aggregator Information

4. 4. 5. 3 State Activity

Click “State Activity”, when you choose Active for port, the port will transmit LACP protocol packets automatically. If not active, will the port respond only when it receives LACP packets from relevant devices.

With two or one positive LACP port, the link will be able to work in dynamic LACP trunking. With two passive LACP ports, the link will not work in dynamic LACP trunking because the two passive ports are waiting for the packets from each other. To activate LACP local end, you have actually set an active status when you choose trunking port.



Port	LACP State Activity	Port	LACP State Activity
1	<input type="checkbox"/> Active	5	<input type="checkbox"/> Active
2	<input type="checkbox"/> Active	6	<input type="checkbox"/> Active
3	<input type="checkbox"/> Active	7	<input type="checkbox"/> Active
4	<input type="checkbox"/> Active	8	<input type="checkbox"/> Active

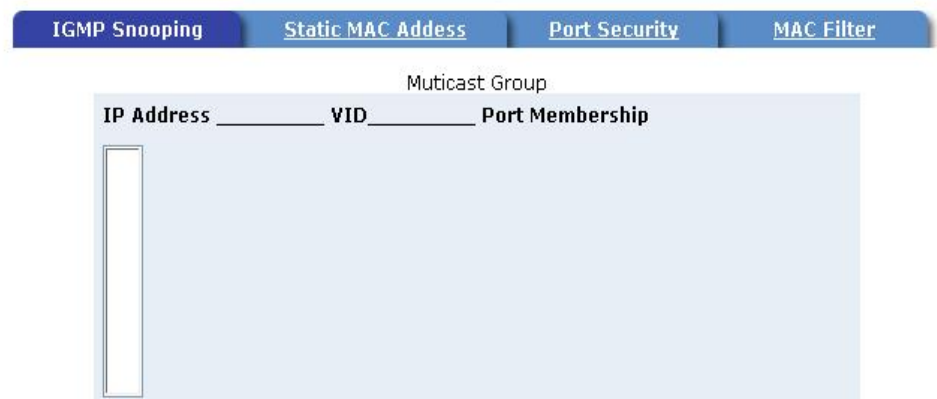
Apply Default Help

Figure4-14 State Activity

4. 4. 6 Filter

4. 4. 6. 1 IGMP Snooping

Click “Administrator” → “Filter”.KIEN5000 and KIEN6000 supports IP multicast. From the page of WEB management “Configuration”→“Advanced”, IGMP protocol can be started up and check the IGMP info. To see different multicast group, the VID and member ports IP multicast address ranges from 224.0.0.0 to 239.255.255.255.



IP Address	VID	Port Membership
------------	-----	-----------------

Figure4-15 IGMP Snooping

Internet Group Management Protocol (IGMP) is an internal protocol of IP station. By supporting IGMP's switch, router and PC, IP manages multicasting. When IGMP is started up, the port can check the query packets and reports packets, and manage IP multicast flow by switch. There are three types of info for IGMP: Query, the message from IGMP router or switch, this message request each PC OF multicast group to send a response; Report, the message PC send to query-maker for indicating the member the PC wants or the message marks; Leave group, the message PC send to query-maker for indicating the PC has left the relevant multicast group.

4. 4. 6. 2 Static MAC Address

Click "Static MAC Address":

IGMP Snooping Static MAC Address Port Security MAC Filter

The follow table list static address of current switch defined .
Click 'Add',you can add a new static entry into the address table.

MAC Address	PORT
-------------	------

MAC Address

Port Number

Vlan ID

Figure4-16 Static MAC Address

When a static MAC address is added, it will stay in the switch's address table for either connection or disconnection between switch and physical devices. When power supply or connection is restart, the switch does not need to study the MAC address. To add as below:

- 1 . Types a MAC address whose flow the port will always forward in the address table.
- 2 . Typing port number.

3 . If a port-based or ID-based VLAN is set up in the switch, the static address will be related to the sole VLAN. Type the VLAN name (port-based or ID based) relevant to MAC address

4 . Click “Add”.

4. 4. 6. 3 Port Security

The port will be locked in security mode and address study is not allowed. Only the SMAC packets in address table can forward normally. You can forbid the port to study any new MAC address and input the MAC address that can use the secure port from the “Static MAC Address” page, click “apply” to activate the change so that prevent illegal visit from end device.

Port	Enable Security (Disable, MAC study)	Port	Enable Security (Disable, MAC study)
1	<input type="checkbox"/>	5	<input type="checkbox"/>
2	<input type="checkbox"/>	6	<input type="checkbox"/>
3	<input type="checkbox"/>	7	<input type="checkbox"/>
4	<input type="checkbox"/>	8	<input type="checkbox"/>

Apply Default Help

Figure4-17 Port Security

4. 4. 6. 4 MAC Filter

MAC filter allow the switch to give up the unwanted packets. Filter packet is based on destination address.

Specified a MAC address to filter.

MAC Address

Mac Address

Vlan ID N/A

Add Delete Help

Figure4-18 MAC Filter

4. 4. 7 VLAN

Virtual LAN (VLAN) is a logical networking group which control broadcast domain. It can isolate the network info and only inform the VLAN member of the message from the same VLAN member. Logically, VLAN among switches is equivalent to re-connect a group of networking devices to another layer-2 switch. Physically, all the networking devices are connected with the same switch.

Default VLAN support is to be enabled and all ports belong to default VLAN, VID is 1.

1 . Port-based VLAN(IEEE 802.1Q VLAN)

Port-based tag rule VLAN is IEEE 802.1Q standard, so it is possible to set up VLAN among devices from different suppliers. IEEE 802.1Q VLAN employs adding tag to Ethernet frame technology. The tag contains VLAN ID (VID) for indicating VLAN quantity.

2 . Protocol-based of VLAN

To enable the end to send packets to different VLANs, the end can either add VLAN tag or is connected to the bridge of a VLAN with tag. The bridge can be based not only default PVID but also other info relevant to packets, such as protocol, to classify the packets and add different VLAN tags.

KIEN5000 and KIEN6000 industrial Ethernet switch supports protocol-based VLAN. It is realized by selecting different general protocol ex: Novell IPX and AppleTalk's Ether Talk, and programmable protocol etc in some degree.

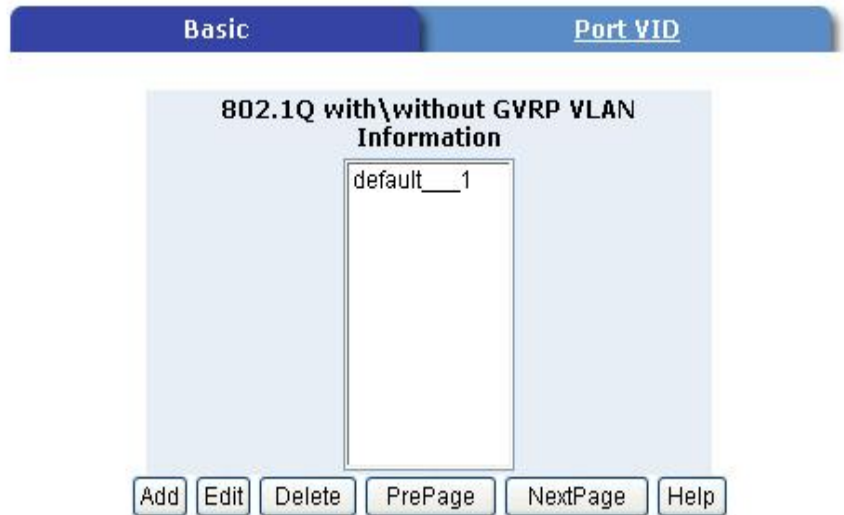


Figure4-19 VLAN

4. 4. 7. 1 Basic



Notes:

“Administrator”→“Configuration”→“Advanced”. You need choose VLAN mode from the page before setting.

Set up 802.1Q with/without GVRP, and add membership port with “tag”:

1. Click “Administrator” → “VLAN “
2. Click “Add”.
3. Name the New VLAN
4. Enter VID (2-4094), Default 1.
5. “Protocol VLAN” can be set as “NONE”.
6. Select port and then click “Add”.
7. Click “Next” and select “tag”.
8. Click “Apply”.

4. 4. 7. 2 Port VID

Click “Port VID” to configure port VID.

Basic
Port VID

Assign a Port VLAN ID (1~4094) for untagged traffic on each port, then click Submit to apply the changes on this page.

No.	PVID	Ingress Filtering 1	Ingress Filtering 2	No.	PVID	Ingress Filtering 1	Ingress Filtering 2
1	1	Enable ▼	Disable ▼	6	1	Enable ▼	Disable ▼
2	1	Enable ▼	Disable ▼	7	1	Enable ▼	Disable ▼
3	1	Enable ▼	Disable ▼	8	1	Enable ▼	Disable ▼
4	1	Enable ▼	Disable ▼	9	1	Enable ▼	Disable ▼
5	1	Enable ▼	Disable ▼	10	1	Enable ▼	Disable ▼

Ingress Filtering Rule 1
(Forward only packets with VID matching this port's configured VID)

Ingress Filtering Rule 2
(Drop Untagged Frame)

Figure4-20 Port VID

Configure the VLAN ID of flow without tag for the given port. Ex: if the default PVID of port 2 is 3, all the packets without tag on port 2 belong to VLAN 3. The default PVID of all ports is set as 1. When you adjust the devices without tag and want to add it into VLAN, this feature is applicable. Each port can only have one VLAN without tag.

✧ Ingress Filtering

Ingress filtering enables the VLAN's frame to be forwarded if the port belongs to VLAN. There are two kind of rules:

Ingress filtering rule 1 : Forward only packets matching the port's VID.

Ingress filtering rule 2 : Drop untagged frame.

4. 4. 7. 3 Advanced

Two situations for you to configure VLANs, one is to divide VLAN in single device and the other one is to divide the VLAN among the devices of the ring network form by KIEN5000 or KIEN6000 switches.

It is simple to divide VLAN in single device; three VLAN modes can all be applied. Just add different VID to different VLAN ports.

When you divide the VLAN in ring network, you need apply 802.1Q with/without GVRP mode. Ex, to form a VLAN as figure below, do as:

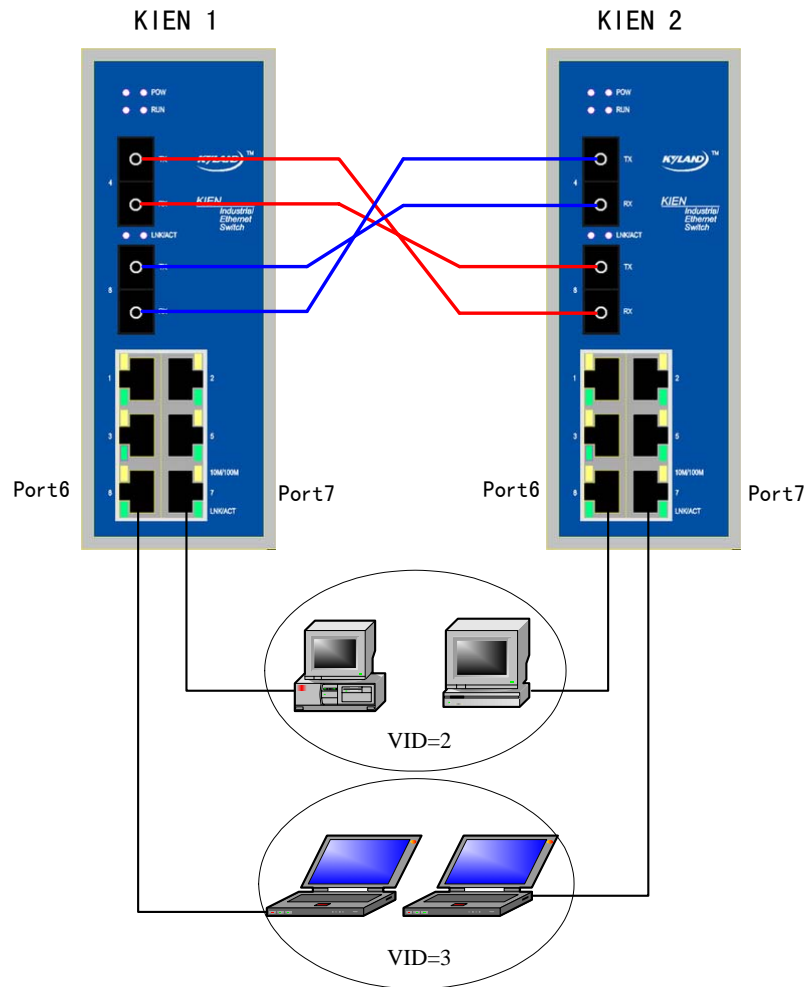


Figure4-21 VLAN in Network

1. Login KIEN1's WEB management, "Administrator" → "Configuration" → "Advanced": 802.1Q with GVRP or 802.1Q without GVRP.
2. Configure VLAN1 including port 4 and 8, VID as 2, Type: tag;
3. Configure VLAN2 including port 4 and 8, VID as 3, Type: tag;
4. According to 4.4.7.2, in page of "Port VID", set as port 6 — PVID 3; port 7 — PVID 2;
5. Login KIEN2's WEB Management, "Administrator" → "Configuration" → "Advanced": 802.1Q with GVRP or 802.1Q without GVRP.
6. Configure VLAN1 including port 4 and 8, VID as 2, Type: tag;
7. Configure VLAN2 including port 4 and 8, VID as 3, Type: tag;
8. According to 4.4.7.2, in page of "Port VID" set as port 6 — PVID

2;; port 7 — PVID 3.

4. 4. 8 STP

Spanning Tree Protocol (STP) is a standard way (IEEE 802.1D) to avoid looping in the switching network. To enable STP is to make sure any two nodes in the network can pass only in one path at one time. In the web management's "switch setting" advanced, you can enable STP.

1 . The following shows information of Root Bridge.

Root Bridge Information	
Priority	32768
Mac Address	000061006039
Root_Path_Cost	0
Root Port	we are root
Max Age	20
Hello Time	2
Forward Delay	15

Figure4-22 Root Bridge Information

2 . The following shows STP port status.

STP Port Status			
PortNum	PathCost	Priority	PortState
1	10	128	DISABLED
2	10	128	FORWARDING
3	10	128	DISABLED
4	10	128	DISABLED
5	10	128	DISABLED
6	10	128	DISABLED
7	10	128	DISABLED
8	10	128	DISABLED
9	10	128	FORWARDING
10	10	128	FORWARDING

Figure4-23 STP Port Status

3 . Configure STP new parameters and click "Apply".

Configure Spanning Tree Parameters

Priority (1-65535)	<input type="text" value="32768"/>
Max Age (6-40)	<input type="text" value="20"/>
Hello Time (1-10)(1-10)	<input type="text" value="2"/>
Forward_Delay_Time(4-30)	<input type="text" value="15"/>

Figure4-24 Configure STP Parameters

The following table shows the meaning of parameters:

Table4-7 STP Parameters

Parameters	Description
Priority	For recognize the value of root bridge. The bridge of smallest value will have the highest priority and be selected as root. Value from 1 to 65535 is valid. To change this value, you need to restart the switch.
Max Age	The time bridge will wait for before it tries to re-configure when it did not receive the news from spanning tree configuration. Value from 6 to 40 is valid.
HELLO time	The interval time to transmit the STP news, valid value is from 1 to 10.
Forward delay time	The time it takes to convert from spanning tree study and monitor status to forward status. Value from 4 to 30 is valid.

4 . Configure all parameters of per-port, and click “Apply”.

Configure Spanning Tree Port Parameters

Port Number	Priority (0 - 255; Default 128)	Path Cost (1 - 65535; Default 10)
<div style="border: 1px solid black; padding: 2px;"> 1 2 3 4 5 </div>	<input type="text" value="128"/>	<input type="text" value="10"/>

Figure4-25 Configure STP Port Parameters

The following table shows the meaning of parameters:

Table4-8 STP Port Parameters

Parameters	Description
Priority	You can set the port as root by setting this value, the value is valid from 0 to 255, and the default is 128, the smaller value, the higher priority. To change the value, you must restart the switch.
Path cost	The path cost of the given port, the switch will know which port is for forwarding through this value. The port with the smallest value will be the forwarding port; the value range is from 1 to 65535. The default value in IEEE 802.1D is 0Mb/s = 50-600; 100Mb/s = 10-60; 1000Mb/s = 3-10. To change this value, you need to restart the switch.

4. 4. 9 Monitor Port

Port sniffer is a way to monitor network flow in the switching network. The flow can be monitored by the given port. The incoming and outgoing monitored flow will be copied to sniffer port.

Roving Analysis State:

Disable

Analysis Port:

None

Monitor Ports	Monitor Rx	Monitor Tx
1	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>

Apply

Default

Help

Figure4-26 Monitor Port

The following table shows the meaning of parameters.

Table4-9 Parameter of Monitor Ports

Item	Description
Roving analysis state	Enabled and disable monitor port
Analysis port	Analysis port is to watch the communication of all monitor ports. You can connect the sniffer port to LAN analyzer or netxray.
Monitor port	The port to be monitored. The flow of all monitored ports will be copied to sniffer port. To invalidate this function, you can select as no monitor ports.
Monitor Rx	Monitor receiving frame of port.
Monitor Tx	Monitor sending frame of port.

4. 4. 10 SNMP

If management information base is installed correctly in the managing end, any management operating SNMP can manage the switch. SNMP is a protocol, which control the information transmission between manager and agent. In our system, SNMPV1 is supported.

You can define the manager PC as trap managers and input SNMP group name in this page. You can also define a name, location and contacts for the switch. Click the “apply” to update this page settings after inputting system data.

Table4-10 SNMP Parameters

Item	Description
Name	Input name of switch.
location	Input location of switch.
Contact	Input personal or community name.

System Options

Name:
Location :
Contact :

Community Strings

urrent Strings :

public__RO
comname__RO

New Community String :
Name
☒ Read Only ☐ Read Write

Trap Managers

Current Managers :

192.168.0.7

New Manager :
IP Address :
Community

Figure4-27 SNMP

Group name can be used as command and input by the way as below:

Item	Description
Read only	Enabled requirement and show MIB information.
Read and write	Enabled requirement, show and configure MIB information.

Trap Managers is the host station to receive traps, which is the system warning generated by switch. If the trap managers are not defined, the traps will not be sent. You can create trap managers by inputting IP address and group name.

4. 4. 11 Security

You can change username and password. Default is :

Username: admin

Password: 123

User Name:	<input type="text" value="admin"/>
Assign/Change password:	<input type="password" value="..."/>
Reconfirm password:	<input type="password" value="..."/>
	<input type="button" value="Apply"/>

Figure4-28 Security

4. 5 TFTP Software Update

You can upgrade software or reboot system remotely:

1. Install TFTP Turbo98 or TFTP Server, and then run it.
2. From [Http://www.kyland.com.cn](http://www.kyland.com.cn) or contact manufacturer to get new software (image.bin) , copy it in TFTP Turbo98.
3. Select “TFTP upgrade” in Web management.
4. Input the host PC’s IP address of TFTP Server software in the IP address bar of TFTP Server.
5. Click “Apply ” to download new document (image.bin), select update software in the web management.

TFTP Server IP Address	<input type="text" value="192.168.0.7"/>
Software File Name	<input type="text" value="image.bin"/>
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

Figure4-29 TFTP software

4. 6 Backup Configuration

4. 6. 1 TFTP Restore Configuration

To make TFTP restore configuration, you also need to run TFTP Turbo98 or other TFIP server software. You can restore the configuration of memory by setting TFTP server address in this page, but first of all, you need to put the backup mirror in the TFTP server and change the default name to flash.dat, so that you can enable the switch to download backup mirror.

TFTP Restore Configuration		TFTP Backup Configuration	
TFTP Server IP Address		192.168.0.7	
Backup File Name		image.bin	
<input type="button" value="Apply"/> <input type="button" value="Help"/>			

Figure4-30 TFTP Restore Configuration



Attention:

The name of the backup file is 11 characters max or five Chinese characters plus one character plus dot.

4. 6. 2 TFTP Backup Configuration

After you have configured TFTP server address and the name of backup file in this page, you can store the EEPROM value and get into TFTP to restore the EEPROM vlues.

TFTP Restore Configuration		TFTP Backup Configuration	
TFTP Server IP Address		192.168.0.7	
Backup File Name		image.bin	
<input type="button" value="Apply"/> <input type="button" value="Help"/>			

Figure4-31 TFTP Backup Configuration

4. 7 Reset

When you click “Reset”, it will be back to default configuration. The following Table4-11 shows all parameters.

Reset Switch to Default Configuration

Figure4-32 Reset System

Table4-11 System Default

Property Name	Size (byte)	Default	Remark
System			
Default data version	1	0x09	
Identity Value	1	0x73	
Mac address	6	0x000060006000	
IP address	4	192.168.0.2	
Sub Mask	4	255.255.255.0	
Gate way	4	192.168.0.1	
Administrator	10	admin	
Password	10	123	
Super username	10	super user	
Super password	10	wio	
Configuration Major Version	1	0x0C	
Configuration Minor Version	1	0x00	
Software Major Version	1	0x00	
Software Minor Version	1	0x37	
TFTP server IP address :192.168.0.1	4	0xC0A80001	
System Description String	32	“IEN 6+2L SWITCH”	
System Name String	32	“IEN 6+2L SWITCH”	
System Position String	32	“6F 531”	
System Content String	32	“6+2 L”	
TRUNK			
LACP priority	2	1	
LACP Value	2	60000	
LACP trunking port quantity	1	8	
LACP Activity State	1	0	Passive
LACP port enable	1	1	Enable
LACP enable	1	1	Enable
Local trunking enabled	1	0	Disable
STP			
STP protocol enabled	1	1	Enable
STP system priority	2	0x8000	
STP max age time	1	15	
STP Hello time	1	3	

STP forwarding delay time	2	5	
STP port priority	1	128	
STP path cost	2	10	
STP port enabled	1	1	Yes
VLAN/GVRP			
VALN port VID	2	1	
VALN ingress rule 1	1	1	Enabled
VALN ingress rule2	1	0	Disable
802.1Q with GVRP VALN	1	1	
Default VALN name	14	“default”	
Default VALN VID	2	0x01	
Default VALN: protocol id = 0	1	0	No
Default VALN number	2	0x3ff	All
Default VALN tagged rule	1	0	None
IGMP			
IGMP protocol enabled	1	1	
Port control			
Port enable	1	0x01	Enabled
Automatism	1	0x01	Enabled
Mega port ability	3	0x18	100M Full duplex
Gega port ability	3	0x1C	1000M Full duplex
Flow control	1	0x01	Enabled
Security	1	0	close
Forwarding			
MAC list aging enable	1	1	Enabled
MAC list aging time	4	300 sec	
QoS Mode	1	WRR	
QoS Policy	1	0xF0	
WRR High Priority Weigh	1	2	
WRR Low Priority Weigh	1	1	
Broadcast Storm filtering	1	Closed	
Transmission Delay Bound	1	1sec	

Time			
Low Priority Queue Delay Bound	1	1	Enabled
Low priority queue delay bound time	1	255ms	
Sniffer		0	Disabled
Analysis port ID		0	
Rx: monitor port shielded		0	
Tx: monitor port shielded		0	
SNMP			
Switch name	128	Empty	
Location description	128	Empty	
Switch contact	128	Empty	
Switch community	128	public	
SNMP Traps IP	16	Empty	
SNMP Traps Group	128	Empty	

4. 8 Reboot

When user reset switch please click “Reboot”.



Figure4-33 Reboot